








BitDefender Version 10

Benutzerhandbuch



Antivirus

Antispyware

Rootkiterkennung





BitDefender Antivirus v10
Benutzerhandbuch

BitDefender



Inhaltsverzeichnis





Endbenutzer Software-Lizenzvertrag

Installieren Sie die Software nicht, wenn Sie diesen Lizenzbedingungen nicht zustimmen. Wenn Sie "Akzeptieren", "OK", "Weiter", "Einverstanden" auswählen, oder wenn Sie sie Software in irgendeiner Form installieren oder nutzen, erklären Sie, dass Sie die Bedingungen des Lizenzvertrages vollständig verstanden und akzeptiert haben.

Diese Bedingungen decken BitDefender Lösungen und Services ab, die wir Ihnen als Anwender lizenziert haben, einschließlich der entsprechenden Dokumentation und aller Updates und Upgrades der Anwendung, die Ihnen unter der gekauften Lizenz oder angeschlossener Service Vereinbarungen geliefert wurden, so wie in der Dokumentation und allen Kopien dieser Vertragsgegenstände festgelegt.

Der Lizenzvertrag und die Gewährleistungsbestimmungen sind ein rechtsgültiger Vertrag zwischen Ihnen (einer natürlichen oder juristischen Person, im Folgenden Benutzer genannt) und der SOFTWIN zur Benutzung des oben und folgend genannten SOFTWIN SOFTWAREPRODUKTES, welches außer dem eigentlichen SOFTWAREPRODUKT auch dazugehörige Medien, gedruckte Materialien und die Nutzung von Online- und anderen Medien oder elektronische Dokumentation (im weiteren bezeichnet BitDefender)beinhaltet. Das SOFTWAREPRODUKT und die zugehörigen Materialien sind durch US-amerikanische Urheberrechtsgesetze und internationale Urheberrechtsverträge geschützt. Indem Sie das SOFTWAREPRODUKT installieren, kopieren, downloaden, darauf zugreifen oder es anderweitig verwenden, erklären Sie sich damit einverstanden, durch die Bestimmungen des Lizenzvertrages und der Gewährleistungsbestimmungen gebunden zu sein. Falls Sie den Bestimmungen dieses Lizenzvertrages und der Gewährleistungsbestimmungen nicht zustimmen, ist der Hersteller SOFTWIN nicht bereit, das SOFTWAREPRODUKT an Sie zu lizenzieren. In diesem Falle sind Sie nicht berechtigt, das SOFTWAREPRODUKT zu verwenden oder zu kopieren.

Installieren oder nutzen Sie BitDefender nicht, wenn Sie dem Lizenzvertrag und den Gewährleistungsbestimmungen nicht zustimmen.

BitDefender Lizenz. Das SOFTWAREPRODUKT ist durch Urheberrechtsgesetze und internationale Urheberrechtsverträge genauso geschützt, wie durch andere Gesetze und Verträge zum Schutz des geistigen Eigentums. Das SOFTWAREPRODUKT wird an Sie lizenziert, nicht verkauft.

LIZENZEINRÄUMUNG: Dieser Vertrag gewährt Ihnen und nur Ihnen eine nicht ausschließliche, eingeschränkte, nicht übertragbare und kostenpflichtige Lizenz BitDefender zu nutzen.

Anwendung der Software. Sie können BitDefender installieren und nutzen, auf so vielen Computern wie nötig, mit der Einschränkung, dass diese Anzahl nicht die Anzahl der lizenzierten Anwender überschreitet. Es kann eine zusätzliche Kopie für ein Back-Up erstellt werden.

Desktop Anwender Lizenz. Diese Lizenz bezieht sich auf BitDefender Software, die auf einzelnen Computern installiert werden kann und keine Netzwerk Eigenschaften hat. Jeder direkte Anwender kann diese Software auf einem einzelnen Computer installieren und zu Back-up Zwecken eine zusätzliche Kopie auf einem anderen Computer erstellen. Die Anzahl der direkten Anwender entspricht der Anzahl der Lizenz Inhaber.

LIZENZBESTIMMUNGEN. Die hiermit gewährte Lizenz ist ab dem Kaufdatum von BitDefender bis zum Ende des Zeitraums, für den die Lizenz erworben wird, gültig.

UPGRADES: Sollte das SOFTWAREPRODUKT BitDefender mit der Bezeichnung Upgrade gekennzeichnet sein, muss der Benutzer für eine berechtigte Nutzung eine gültige, von SOFTWIN als berechtigte für BitDefender anerkannte, Softwarelizenz haben. Das als Upgrade gekennzeichnete SOFTWAREPRODUKT BitDefender ersetzt und / oder ergänzt das zum Upgrade berechtigende BitDefender. Der Benutzer darf das aus dem Upgrade resultierende SOFTWAREPRODUKT nur nach dem hier vorliegenden Lizenzvertrag nutzen. Sollte das als Upgrade gekennzeichnete BitDefender ein Upgrade für eine einzelne Komponente eines kompletten Softwarepaketes sein, darf das SOFTWAREPRODUKT BitDefender auch nur als einzelner Bestandteil dieses

Softwarepaketes genutzt und transferiert werden und darf nicht als separates Produkt auf mehr als einem Einzelplatzrechner genutzt werden. Die Geschäftsbedingungen dieser Lizenz ersetzen und lösen alle vorangehenden Vereinbarungen ab, die zwischen Ihnen und Softwin bestanden haben in Bezug auf das Original Produkt und das daraus resultierende Upgrade Produkt.

URHEBERRECHT: Alle Rechte und geistigen Eigentumsrechte an BitDefender(einschließlich, aber nicht beschränkt auf Logos, Bilder, Fotografien, Animationen, Video, Audio, Musik, Text und "Applets", die in BitDefender enthalten sind), den gedruckten Begleitmaterialien und jeder Kopie von BitDefender liegen bei SOFTWIN. Das BitDefender ist durch anwendbare Urheberrechtsgesetze und andere Gesetze und Vereinbarungen über geistiges Eigentum geschützt. Darum muss der Benutzer BitDefender wie jedes andere urheberrechtliche Produkt behandeln, mit der Ausnahme, dass er BitDefender auf einem Einzelplatzrechner installieren und das Original zu Sicherungszwecken speichern darf. Der Benutzer darf die zugehörigen, gedruckten Materialien nicht vervielfältigen. Der Benutzer muss BitDefender als Ganzes, wie erhalten, inklusiver aller Urheberrechtsvermerke und aller zugehörigen Materialien und Medien in der ihm vorliegenden Form bewahren. Der Benutzer ist nicht berechtigt, BitDefender weiter zu lizenzieren, zu vermieten, zu verleihen und / oder zu verkaufen. Der Benutzer darf BitDefender nicht zurückentwickeln (Reverse Engineering), dekompilieren, disassemblieren, daraus Derivate erzeugen, modifizieren, übersetzen oder irgendeinen anderen Versuch starten, den Quellcode von BitDefender freizulegen.

EINGESCHRÄNKTE GEWÄHRLEISTUNG: SOFTWIN gewährleistet für einen Zeitraum von 30 Tagen, dass das Medium auf dem BitDefender geliefert wird, frei von allen Defekten ist. Sollte dies nicht der Fall sein, wird SOFTWIN das Medium austauschen oder dem Benutzer den Betrag zurück erstatten, den der Benutzer für BitDefender bezahlt hat. SOFTWIN gewährleistet weder die dauerhafte Verfügbarkeit, noch die Fehlerfreiheit von BitDefender, noch dass Unzulänglichkeiten und Fehler von BitDefender behoben werden. SOFTWIN gewährleistet ebenso nicht, dass BitDefender den Anforderungen des Benutzers entspricht.

SOFERN IN DER VORLIEGENDEN VEREINBARUNG NICHT AUSDRÜCKLICH ANDERWEITIG FESTGELEGT, LEHNT SOFTWIN ALLE ANDEREN AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN IM HINBLICK AUF DIE PRODUKTE, DAMIT ZUSAMMENHÄNGENDE VERBESSERUNGEN, WARTUNG ODER SUPPORT ODER ALLE ANDEREN VON SOFTWIN GELIEFERTEN (MATERIELLEN ODER IMMATERIELLEN) MATERIALIEN ODER ERBRACHTEN DIENSTLEISTUNGEN AB. SOFTWIN LEHNT HIERMIT AUSDRÜCKLICH ALLE STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN UND ZUSICHERUNGEN AB, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE GEWÄHRLEISTUNG WEGEN RECHTSMÄNGEL, DIE GEWÄHRLEISTUNG DER NICHT-KOLLISION, DER GENAUIGKEIT VON DATEN UND INFORMATIONEN, DER SYSTEMINTEGRATION UND DER NICHTVERLETZUNG VON RECHTEN DRITTER DURCH DAS FILTERN, DEAKTIVIEREN ODER ENTFERNEN VON FREMDANBIETERSOFTWARE, SPYWARE, ADWARE, COOKIES, E-MAILS, DOKUMENTEN, ANZEIGEN ODER ÄHNLICHEM, UNABHÄNGIG DAVON, OB DIES AUFGRUND GESETZLICHER ANFORDERUNGEN, DER GESCHÄFTSTÄTIGKEIT, DES GEWOHNHEITSRECHTS UND DER PRAXIS ODER DES HANDELSGEBRAUCHS ERFOLGT.

BESCHRÄNKUNG DER HAFTUNG: Jeder Benutzer von BitDefender, der dieses benutzt, testet oder auch nur ausprobiert trägt alleinig das Risiko, das aus der Qualität und Performance von BitDefender entsteht. In keinem Fall können SOFTWIN oder ihre Lieferanten auf irgendeine Weise für, durch Verwendung von BitDefender, entstandene Schäden jeder Art haftbar gemacht werden, einschließlich und ohne Beschränkung, direkter und indirekter, zufälliger und spezieller Schäden die aus der Verwendung, Performance oder der Verfügbarmachung von BitDefender entstanden sind. Dies gilt auch dann, wenn SOFTWIN über existierende und / oder mögliche Schäden informiert wurde. IN KEINEM FALL KÖNNEN SCHADENSERSATZANSPRÜCHE IN EINER HÖHE GELTEND GEMACHT WERDEN, DIE DEN KAUFPREIS DES SOFTWAREPRODUKTES ÜBERSTEIGEN. Alle Erklärungen und Beschränkungen behalten auf jeden Fall ihre Gültigkeit unabhängig von der Nutzungsart (reguläre Benutzung, Test, etc.).



Wichtige Informationen für die Anwender. WICHTIGE INFORMATION FÜR DEN BENUTZER: DIESES SOFTWAREPRODUKT IST NICHT FEHLERTOLERANT UND IST AUCH NICHT FÜR EINE NUTZUNG IN KRITISCHEN UMGEBUNGEN, IN DENEN ES AUF EINE AUSFALLSICHERE PERFORMANCE UND BEDIENUNG ANKOMMT, KONZIPIERT UND ERSTELLT. DIESES SOFTWAREPRODUKT IST NICHT GEEIGNET ZUR NUTZUNG IM LUFTVERKEHR, IN NUKLEARKRAFTWERKEN, IN KOMMUNIKATIONSSYSTEMEN, IN WAFFENSYSTEMEN, IN DIREKTEN ODER INDIREKTEN LEBENSERHALTUNGSSYSTEMEN ODER IRGENDEINEM ANDEREN SYSTEM, DESSEN AUSFALL ZU TODESFÄLLEN, KÖRPERLICHEN SCHÄDEN ODER VERMÖGENSSCHÄDEN FÜHREN KÖNNTE.

Allgemein. Dieser Vertrag unterliegt dem Recht von Rumänien, internationalen Copy Right Bestimmungen und Abkommen.

Preise, Kosten und Gebühren für die Nutzung von BitDefender gelten vorbehaltlich von Änderungen auch ohne vorherige Information.

Ist oder wird eine Bestimmung dieses Vertrageswegen Verstoßes gegen zwingende gesetzliche Bestimmungen unwirksam oderwird sie für unwirksam erklärt, so wird hierdurch die Gültigkeit des übrigen, mitder unwirksamen Bestimmung nicht unmittelbar zusammenhängenden Vertragsteils,nicht berührt.

BitDefender und alle zugehörigen Logos sind eingetrageneTitel und Marken von SOFTWIN. Alle anderen Marken und Titel sind Eigentumder jeweiligen Rechteinhaber.

Wenn Sie gegen eine Lizenzbestimmung verstoßen, wird die Lizenz unverzüglich fristlos beendet. Sie haben aufgrund der Beendigung keinen Anspruch auf eine Erstattung von SOFTWIN oder einem Händler von BitDefender. Die Bestimmungen im Hinblick auf Geheimhaltung und Beschränkungen gelten über die Laufzeit der Lizenz hinaus.

SOFTWIN ist berechtigt, die vorliegenden Bestimmungen jederzeit zu überarbeiten. Die überarbeiteten Bestimmungen gelten automatisch für die entsprechenden Software-Versionen, die mit den geänderten Bestimmungen geliefert werden. Sollte eine der vorliegenden Bestimmungen ungültig und nicht durchführbar sein, bleibt die Gültigkeit der übrigen Bestimmungen davon unberührt.

Im Fall von Widersprüchen oder Unstimmigkeiten zwischen übersetzten Fassungen der vorliegenden Bestimmungen gilt die von SOFTWIN ausgegebene englische Fassung.

Kontakt SOFTWIN, at 5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Romania, or at Tel No: 40-21-2330780 or Fax:40-21-2330763, e-mail address: `<office@bitdefender.com>`.



Vorwort

Dieses Benutzerhandbuch ist für alle Benutzer vorgesehen, die sich für **BitDefender Antivirus v10** als Sicherheitslösung entschieden haben. Die in diesem Dokument beschriebenen Informationen sind nicht nur für IT-Profis gedacht, sondern auch für all diejenigen die sich nur in Ihrer Freizeit mit dem Computer beschäftigen.

Es wird beschrieben wie **BitDefender Antivirus v10** zu handhaben ist, wie das Produkt optimal konfiguriert werden kann und wie Sie die Einstellungen Ihren Bedürfnissen anpassen können. So lernen Sie optimal mit diesem Produkt umzugehen und es effektiv einzusetzen.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

1. Verwendete Konventionen

1.1. Typografie

Um die Lesbarkeit zu fördern werden verschiedene Arten von Textstilen verwendet. Die jeweiligen Bedeutungen entnehmen Sie bitte der Tabelle unterhalb.

Erscheinungsbild	Beschreibung
`sample syntax`	Syntaxbeispiele werden in einer Schriftart mit `fester Laufweite` angegeben.
http://www.bitdefender.com	Verweise (Links) auf externe Inhalte wie z.B. Webseiten oder FTP-Server.
`<support@bitdefender.com>`	Verweise auf E-Mail-Adressen, z.B. zur Kontaktaufnahme.
„Vorwort“ (S. xi)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
`filename`	Dateien und Verzeichnisse werden in einer Schriftart mit `fester Laufweite` angegeben.
option	Optionen wie z.B. Schaltflächen oder Checkbox- Elemente werden in **fett gedruckt** angegeben.
`sample code listing`	Beispielquelltexte werden in einer Schriftart mit `fester Laufweite` angegeben.

1.2. Warnungen

Bei diesen Symbolen handelt es sich um Hinweise innerhalb des Textflusses welche mit einer kleinen Grafik markiert sind. Hierbei handelt es sich um Informationen die Sie in jedem Fall beachten sollten.



Anmerkung

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.



Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.



Warnung

Diese kritische Information sollten Sie mit höchster Aufmerksamkeit verfolgen. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst prekäre Thematik handelt.

2. Struktur

Dieses Handbuch ist in sieben Abschnitte unterteilt, welche die folgenden Hauptthemen beinhalten: Über BitDefender, Installation von BitDefender, Beschreibung und Bestandteile, Die Management Konsole, Tipps und Tricks, BitDefender Notfall CD und Hilfe erhalten. Des Weiteren beinhaltet dieses Dokument ein Glossar und Anhänge um den ein oder anderen Aspekt zu klären, der sonst ggf. zu technischen Problemen führen könnte.

Über BitDefender. Eine kurze Einführung zu BitDefender und SOFTWIN, der Firma hinter diesem Produkt.

Produktinstallation. Schritt-für-Schritt Anleitung zur Installation von BitDefender auf Ihrem Computer. Hierbei erhalten Sie ausführliche Informationen für eine erfolgreiche Installation von **BitDefender Antivirus v10** und werden durch jeden Schritt begleitet. Zusätzlich wird beschreiben wie eine Deinstallation von BitDefender durchzuführen ist.

Beschreibung und Funktionen. **BitDefender Antivirus v10**, Eigenschaften und Module.

Konfiguration. Beschreibt die einfache Verwaltung und Konfiguration von BitDefender. Dieser Abschnitt erklärt wie das **BitDefender Antivirus v10** zu registrieren ist, wie ein Prüfvorgang durchgeführt werden kann und wie ein Update von BitDefender durchgeführt werden kann.

Empfohlene Vorgehensweisen. Folgen Sie den angegebenen Schritten und Anweisungen um BitDefender bestmöglich zu nutzen.

BitDefender Notfall CD. Beschreibung der BitDefender Notfall CD. Erläutert die Funktionen und den Einsatz der startfähigen CD.

Hilfe erhalten. Beschreibt wie Sie Hilfe bzw. Unterstützung zu dem Produkt erhalten und erhält zusätzlich eine Liste mit den am häufigsten gestellten Fragen (FAQ).

Glossar. Im Glossar werden technische Ausdrücke und seltene Bezeichnungen erklärt, die in diesem Dokument zu finden sind.

3. Ihre Mithilfe

Wir laden Sie dazu ein uns bei der Verbesserung dieses Dokuments mitzuhelfen. Wir haben sämtliche Informationen in diesem Dokument bestmöglich überprüft um somit die Qualität sicherzustellen.

Falls Sie dennoch Fehler finden, so teilen Sie uns diese bitte mit indem Sie uns per E-Mail unter der Adresse `<documentation@bitdefender.com>` kontaktieren.



Wichtig

Bitte verfassen Sie alle auf die Dokumentation bezogenen E-Mails auf Englisch.



1. Was ist BitDefender?

BitDefender ist einer der weltweit führenden Hersteller von Sicherheitslösungen und bietet eine der schnellsten und höchst effizienten Sicherheitslösungen in diesem Industriesegment an. Produkte und Dienstleistungen von BitDefender kommen in über 41 Millionen Haushalten und Firmen in mehr als 180 Ländern weltweit zum Einsatz. BitDefender unterhält Büros in den **Vereinigten Staaten**, in **Großbritannien**, **Deutschland**, **Spanien** und **Rumänien**.

- Features: Antivirus, Firewall, Antispyware, Antispam, und Kindersicherung.
- Die BitDefender Produktreihe ist daraufhin ausgelegt in komplexen IT Strukturen (Work Stations, File Servers, Mail Servers und Gateways)implementiert zu werden und zwar für Windows, Linux und FreeBSD.
- Weltweite Distribution, Produkte in 18 Sprachen verfügbar;
- Einfache Bedienbarkeit kombiniert mit einem Installationsassistent welcher den lediglich Benutzer vereinzelte Fragen stellt;
- Internation zertifizierte Produkte: Virus Bulletin, ICSA Labs, Checkmar, IST Prize, usw;
- Rund um die Uhr Kundenbetreuung - 24 Stunden am Tag, 7 Tage die Woche;
- Blitzschnelle Reaktionszeiten beim Bereitstellen von Virensignaturen zur Bekämpfung von Schädlingen;
- Beste Erkennungsraten;
- Stündliche Updates für Virensignaturen - automatisch oder geplante Aktionen schützen vor neuen Viren und anderen Schädlingen.

1.1. Warum BitDefender?

Bewährt: Der reaktionsfähigste Hersteller von AntiViren-Produkten. Die Reaktionsfähigkeit von BitDefender wurde bereits bei den Ausbrüchen von CodeRed, Nimda, Sircam, Badtrans.B und weiteren Schädlingen auf die Probe gestellt. BitDefender war das erste AntiViren-Produkt welches effektive Gegenmittel, sog. „Removal Tools“, für die genannten Schädlinge bereitstellte und dies vollkommen kostenlos für Benutzer auf der ganzen Welt. Mit der kontinuierlichen Verbreitung immer neuer Schädlinge und Varianten gehört der effiziente Schutz vor solchen Bedrohungen mittlerweile zu einem „Must have“ für diejenigen, die tagtäglich mit Computersystemen arbeiten.

Innovation: Ausgezeichnet von der Europäischen Kommission und EuroCase. BitDefender wurde zum Gewinner des europäischen IST-Prize gekürt, welcher von der Europäischen Kommission und Vertreten von 18 Akademien in ganz Europa vergeben wird. Seit acht Jahren vergeben zählt der IST-Prize mittlerweile als Auszeichnung für wegweisende Innovationen und repräsentiert somit die beste Innovation der europäischen Informationstechnologie.

Umfassend: Sichert Einstiegspunkte im Netzwerk und bietet effektiven Schutz. Sicherheitslösungen mit BitDefender werden den Anforderungen in Unternehmensnetzwerken mehr als gerecht. Sie sind nicht nur geeignet für den Einsatz in kleinen und mittelständischen Unternehmen sondern auch in Multi-Plattform Netzwerken weltweit agierender Konzerne bietet BitDefender effektiven Schutz. Somit wird sichergestellt, dass Viren und andere Schädlinge erst gar keine Möglichkeit erhalten sich in Unternehmensnetzwerken zu verbreiten.

Optimaler Schutz: Sicherheit vor Bedrohungen auf Ihrem Computer. Da Virenerkennung basierend auf Quellcode-Analyse lange nicht mehr ausreicht um Schädlinge ausreichend früh zu erkennen, arbeitet das Team von BitDefender stets an neuen Technologien zur frühzeitigen Erkennung von Schädlingen und pro-aktivem Schutz vor diesen.

Sicherheitsprodukte wurden geschaffen um in Firmen, Einrichtungen und bei Privatpersonen die folgenden **möglichen Schäden** zu verhindern:

- Wurm-Angriffe
- Störung der Kommunikation durch infizierte E-Mails
- Zusammenbrechen von Servern
- Desinfizierung und Wiederherstellung von Computersystemen
- Produktivitätsverlust durch nicht verfügbare Systeme
- Cracking und unautorisierte Zugriffe auf sensible Daten

Durch die stetige Weiterentwicklung und den pro-aktiven Schutz von BitDefender können die folgenden **Vorteile** gesichert werden:

- Verbesserte Netzwerkverfügbarkeit durch rechtzeitige Unterbindung von Wurm- Angriffen.
- Schutz der Remote-Benutzer und Clients vor Viren-Angriffen.
- Minimierung des administrativen Aufwands und der Kosten durch Remote- Management Funktionalität der BitDefender-Produkte.
- Unterbindung der Verbreitung von Viren und anderen Schädlingen durch den Schutz der zentralen Kommunikationswege wie Fileserver, E-Mail-Server und Gateways mittels BitDefender.

Weitere Informationen über BitDefender erhalten Sie unter:www.bitdefender.de

1.2. Über SOFTWIN

Im Jahre 1990 gegründet und Gewinner des Europäischen IST-Prize in 2002, wird Softwin mittlerweile als führend in der Osteuropäischen Softwareindustrie angesehen, mit einer Zuwachsrate von 50% in den letzten 5 Jahren und 70 % Exportanteil am Jahreumsatz.

Mit einem Team von mehr als über 800 qualifizierten Mitarbeitern und mehr als 1000 Projekten bislang hat SOFTWIN es sich zur Aufgabe gemacht, Sicherheitslösungen und -dienste bereitzustellen, die den heutigen Anforderungen von schnell expandieren Firmen im Bereich IT-Sicherheit entsprechen und diesen Vorsprung auszubauen. Der Entwicklungsprozess bei Softwin ist ISO 9001 zertifiziert.

Da Softwin in den weit entwickelten IT Märkten in den USA und Europa aktiv ist gibt es 4 verbundene **Geschäftsbereiche** :

- eContent Solutions
- BitDefender
- Business Information Solutions
- Customer Relationship Management



2. Installation von BitDefender Antivirus v10

Der Abschnitt **Installation von BitDefender Antivirus v10** beschreibt die folgenden Themen:

- Systemanforderungen
- Installationsschritte
- Der Regelassistent
- Upgrade von einer vorherigen Version
- Ändern, Reparieren, Deinstallieren

2.1. Systemanforderungen

Für den sachgemäßen und fehlerfreien Betrieb sollten Sie vor der Installation sicherstellen, dass die folgenden Systemanforderungen erfüllt sind:

Microsoft Windows 98 SE, Me, NT (inkl. SP6), 2000 oder XP (32-Bit)

- Pentium II 350 MHZ oder höher
- 128 MB Arbeitsspeicher (256 MB empfohlen)
- 60 MB freier Speicherplatz auf der Festplatte
- Internet Explorer 5.5 (oder höher)

Microsoft Windows Vista (32-Bit)

- 800 MHz oder schneller
- 512 MB Arbeitsspeicher (1 GB empfohlen)
- 60 MB freier Speicherplatz auf der Festplatte

BitDefender Antivirus v10 kanne von der Internetseite http://www.bitdefender.de heruntergeladen werden. Die Internetseite für Ihre Sicherheit.

2.2. Installationsschritte

Lokalisieren Sie die Setup-Datei und führen Sie einen Doppelklick aus. Sie starten damit einen Assistenten, der Sie durch den Installationsprozess leitet.

Installationsschritte

1. Klicken Sie auf **Weiter**, um fortzufahren, oder klicken Sie auf **Abbrechen**, um die Installation abzubrechen.
2. Klicken Sie auf **Weiter** um fortzufahren, oder auf **Zurück** um wieder zum ersten Schritt zu gelangen.
3. BitDefender v10 informiert Sie sofern weitere Antiviren-Produkte auf Ihrem Computer installiert sind.



Warnung

Es wird dringend empfohlen andere Antiviren-Programme zuvor zu deinstallieren. Eine zeitgleiche Verwendung mehrerer Antiviren-Produkte kann Instabilität und Systemabstürze zur Folge haben.

Klicken Sie auf **Zurück**, um zum letzten Schritt zurückzukehren, oder klicken Sie auf **Weiter**, um mit dem Assistenten fortzufahren.



Anmerkung

Falls BitDefender v10 keine weiteren Antiviren-Produkte auf diesem Computer erkennt wird dieser Schritt übersprungen.



4. Lesen Sie die Lizenzbedingungen, wählen Sie die Option **Ich stimme den Lizenzbedingungen zu**, und klicken Sie auf **Weiter**. Wenn Sie den Lizenzbestimmungen nicht zustimmen, klicken Sie auf **Abbrechen**. Der Installationsprozess wird abgebrochen und das Setup-Programm beendet.
5. Sie können bei der Installation zwischen verschieden Arten wählen: Normal, Benutzerdefiniert oder Vollständig.

   Typisch

   Das Programm wird mit den gebräuchlichen Einstellungen installiert. Dies ist die für die meisten Nutzer empfohlene Einstellung.

   Benutzerdefiniert

   Sie können die Einstellungen wählen, wenn Sie benutzerdefiniert installieren möchten. Diese Option wird nur erfahrenen Benutzern empfohlen.

   Vollständig

   Vollständige Installation. Alle Komponenten des Programms werden installiert.

   Wenn Sie **Typisch** oder **Vollständig** gewählt haben, überspringen Sie Schritt 6.
6. Wenn Sie **Benutzerdefiniert**, gewählt haben, öffnet sich ein Fenster mit allen BitDefender Komponenten, so dass Sie aus einer Liste wählen können, was Sie installieren möchten.

   Wenn Sie auf einen Komponentennamen klicken, wird auf der rechten Seite eine kurze Beschreibung angezeigt (in der auch der minimal erforderliche Festplattenplatz für die gewählte Option angegeben wird). Wenn Sie auf das Symbol einer Komponente klicken, wird ein Fenster angezeigt, in dem Sie die Auswahl bestätigen oder verwerfen können.

   Sie können den Ordner wählen, in dem das Produkt installiert werden soll. Standardmäßig wird BitDefender im Ordner `C:\Programme\Softwin\BitDefender 10` installiert.

   Falls Sie einen anderen Ordner wählen möchten, klicken Sie auf **Durchsuchen** und ein neues Fenster wird geöffnet, wo Sie einen neuen Ordner wählen können. Klicken Sie auf **Weiter**.
7. Sie haben zwei Möglichkeiten:
   - **Öffnen der Readme Datei** - öffnen der Readme Datei am Ende der Installation.
   - **Verknüpfung auf dem Desktop erstellen** - um ein Symbol am Ende der Installation auf Ihrem Desktop zu speichern.

   Klicken Sie auf **Installieren**, um mit der Installation des Produkts zu beginnen.

   Wichtig

   Während der Installation erscheint ein Assistent. Dieser hilft Ihnen **BitDefender Antivirus v10**zu registrieren, ein BitDefender Nutzeraccount einzurichten und wichtige BitDefender Sicherheitseinstellungen vorzunehmen.
   Vervollständigen Sie den Assistenten um zum nächsten Schritt zu gelangen.
8. Klicken Sie auf **Fertigstellen**, um die Installation abzuschließen. Wenn Sie die standardmäßigen Einstellungen für die Installation akzeptiert haben, wurde ein neuer Ordner mit dem Namen `Softwin` in `Programme Dateien` angelegt, der den Unterordner `BitDefender 10` beinhaltet.

   Anmerkung

   Sie werden aufgefordert, Ihren Computer neu zu starten, damit der Setup-Assistent das Setup beenden kann.

2.3. Einrichtungs-Assistent

Während der Installation erscheint Assistent. Der Assistent hilft Ihnen **BitDefender Antivirus v10**zu registrieren, ein BitDefender Nutzeraccount einzurichten und wichtige BitDefender Sicherheitseinstellungen vorzunehmen.

Ist ist nicht erforderlich den Assistenten abzuschließen. Dennoch empfehlen wir es Ihnen um Ihr System zu sichern noch bevor BitDefender vollständig installiert wurde.

2.3.1. Schritt 1/8 - Willkommen zum BitDefender Einrichtungs-Assistent



Begrüßungsfenster

Klicken Sie auf **Weiter**.

2.3.2. Schritt 2/8 - BitDefender registrieren



Registrierung

Wählen Sie **Produkt registrieren** um **BitDefender Antivirus v10** zu registrieren. Geben Sie im Feld **neuen Lizenzschlüssel eingeben** den Lizenzschlüssel ein.

Um das Produkt weiter zu testen, klicken Sie bitte auf die Schaltfläche **Produkt weiter testen**.

Klicken Sie auf **Weiter**.



2.3.3. Schritt 3/8 - BitDefender Benutzerkonto erstellen



Kontoerstellung

Ich habe noch kein BitDefender Benutzerkonto

Um vom technischen Support von BitDefender zu profitieren und weitere zur Verfügung stehende Services zu erhalten müssen Sie ein Nutzerkonto einrichten.

Tragen Sie eine gültige E-Mail Adresse **E-mail** in das Feld ein. Legen Sie ein Passwort fest und geben es in das Feld **Password** ein. Bestätigen Sie das Passwort **durch Wiederholen** . Zum Einloggen in Ihr Nutzerkonto benutzen Sie Ihre E-Mail und das Passwort http://myaccount.bitdefender.com.

Anmerkung
Das Passwort sollte mindestens 4 Zeichen haben.

Um erfolgreich ein Nutzerkonto einzurichten müsssen Sie zunächste Ihre E-Mail Adresse aktivieren. Überprüfen Sie Ihre E-Mail Adresse und folgen Sie den Instruktionen, die Ihnen per E-Mail vom BitDefender Registrierungsservice zugeschickt wurden.



Wichtig
Bitte aktivieren Sie Ihr Nutzerkonto bevor Sie zum nächsten Schritt weitergehen.

Wenn Sie kein BitDefender Nutzerkonto einrichten wollen, klicken Sie auf **Diesen Schritt überspringen**. Überspringen Sie ebenfalls den nächsten Schritt des Assistenten.

Klicken Sie auf **Weiter**. Wenn Sie auf **Abbrechen** klicken, wird der Assistent beendet.

Ich habe bereits ein BitDefender Nutzerkonto.

Wenn Sie bereits ein aktives Nutzerkonto haben, geben Sie Ihre E-Mail und das Passwort ein. Wenn Sie ein falsches Passwort eingeben, werden Sie zur Wiederholung aufgefordert, wenn Sie auf **Weiter** klicken. Klicken Sie **Ok** um das Passwort nochmal einzugeben oder **abbrechen** um den Assistenten zu beenden.

Wenn Sie Ihr Passwort vergessen haben, klicken Sie **Passwort vergessen?** und folgen Sie den Instruktionen.

Klicken Sie auf **Weiter**. Wenn Sie auf **Abbrechen** klicken, wird der Assistent beendet.

2.3.4. Schritt 4/8 – Daten Nutzerkonto eingeben



Daten Nutzerkonto



Anmerkung

Sie können den Schritt auslassen, wenn Sie **Diesen Schritt auslassen anklicken** in dem Feld Schritt Drei.

Tragen Sie bitte Ihren Vor- und Nachnahmen ein und wählen Sie ein Land aus.

Wenn Sie bereits ein Benutzerkonto haben wird der Assistent Ihnen die bereits eingetragenen Informationen anzeigen, falls Sie Daten hinterlegt haben. Sie können hier Änderungen vornehmen.

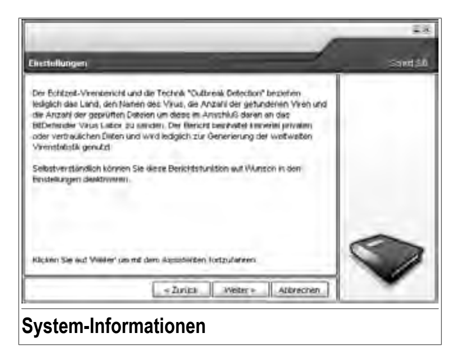


Wichtig

Die hier eingetragenen Daten bleiben vertraulich.

Klicken Sie auf **Weiter**. Wenn Sie auf **Abbrechen** klicken, wird der Assistent beendet.

2.3.5. Schritt 5/8 - Informationen über RTVR

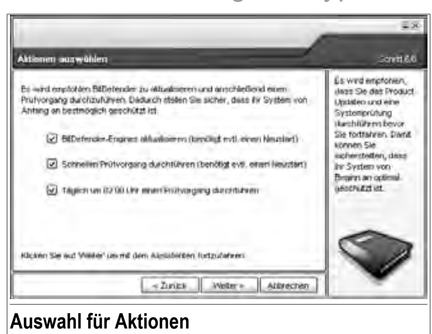


System-Informationen

Klicken Sie auf **Weiter**. Wenn Sie auf **Abbrechen** klicken, wird der Assistent beendet.



2.3.6. Schritt 6/8 – Aufgabentyp



Auswahl für Aktionen

Nehmen Sie hier die BitDefender Sicherheitseinstellungen für Ihr System vor.

Folgende Optionen stehen zur Verfügung:

- **Update der BitDefender v10 Engines (möglicherweise mit Neustart)** - beim nächsten Schritt wird ein Update der BitDefender Engine durchgeführt, um Ihren Computer gegen aktuelle Gefahren zu schützen.
- **Schnelle Systemprüfung (erfordert möglicherweise Neustart)** - Während des nächsten Schrittes wird eine Schnellprüfung durchgeführt, damit BitDefender sicherstellen kann, dass Ihre Dateien aus dem Verzeichnis `Windows` and `Program Files` nicht infiziert werden.
- **Jeden Tag um 02:00 Uhr einen Prüfvorgang ausführen** - führt jeden Freitag zur angegebenen Uhrzeit einen Prüfvorgang aus.



Wichtig

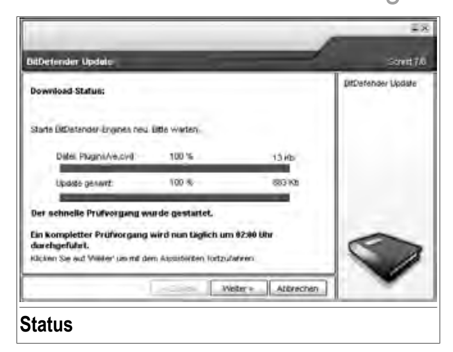
Wir empfehlen die Aktivierung dieser Optionen um die optimale Sicherheit Ihres Systems zu gewährleisten.

Wenn sie keine der Optionen oder nur die letzte auswählen wird der nächste Schritt übersprungen.

Sie können jedoch jegliche Veränderungen vornehmen, in dem Sie zu den vorherigen Schritten zurückkehren (Klicken Sie auf **Zurück**). Weiterhin, ist dieses Verfahren nicht umkehrbar: falls Sie fortsetzen auswählen, wird es nicht möglich sein zu den vorherigen Schritten zurückzukehren.

Klicken Sie auf **Weiter**. Wenn Sie auf **Abbrechen** klicken, wird der Assistent beendet.

2.3.7. Schritt 7/8 - Warten bis Aufgaben vervollständigt wurden

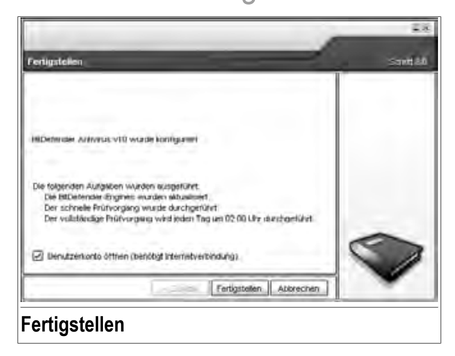


Status

Warten bis die Aufgaben vervollständigt wurden. Sie können den Status der Aufgaben nun sehen.

Klicken Sie auf **Weiter**. Wenn Sie auf **Abbrechen** klicken, wird der Assistent beendet.

2.3.8. Schritt 8/8 – Aufgabenübersicht



Fertigstellen

Dies ist der letzte Schritt der Konfigurationsassistenten.

Klicken Sie in der BitDefender Management-Konsole auf die Option **Berichte**

Klicken Sie auf **Fertigstellen**, um den Installations-Assistent abzuschliessen und mit der Installation fortzusetzen.

2.4. Upgrade

Die Prozedur für das Upgrade kann über zwei Schritte erfolgen:

- Installation ohne die Vorgängerversion zu deinstallieren – nur beim Upgrade von v8 oder höher, ausschließlich Internet Security.



Doppelklick auf die Setup–Datei und folgen Sie bitte dem Assistenten wie beschrieben im Abschnitt „*Installationsschritte*“ (S. 3).



Wichtig

Während des Installationsprozesses erscheint eine Fehleranzeige beruhend auf dem `FILESpy-Dienst`. Bitte klicken Sie auf **OK**, um mit der Installation fortzufahren.

- **Deinstallieren Sie bitte die Vorgängerversion und installieren Sie die neue Version. Dies gilt für alle BitDefender Versionen.**

  Deinstallieren Sie zunächst die Vorgängerversion. Starten Sie dann den Computer neu und installieren Sie die neue Version wie im Abschnitt „*Installationsschritte*“ (S. 3) beschrieben.



Wichtig

Nach dem Upgrade können sämtliche Einstellungen wieder geladen werden.

2.5. Entfernen, reparieren oder ändern einzelner BitDefender Funktionen

Wenn Sie das Programm **BitDefender Antivirus v10** ändern, reparieren oder entfernen möchten, gehen Sie über das Windows-Startmenü wie folgt vor: **Start** → **Programme** → **BitDefender Antivirus v10** → **Ändern, Reparieren oder Deinstallieren**

Sie werden aufgefordert, Ihre Auswahl zu bestätigen. Klicken Sie dazu auf **Weiter**. Ein neues Fenster mit folgenden Auswahloptionen wird angezeigt:

- **Ändern** - dient zum Hinzufügen bzw. Entfernen von Programmkomponenten;
- **Reparieren** - dient zur Neuinstallation sämtlicher Programmkomponenten, die beim vorhergegangenen Setup installiert wurden;



Wichtig

Nach dem Reparaturvorgang können alle Einstellungen wieder geladen werden.

- **Entfernen** - dient zum Entfernen aller installierten Komponenten.

Um mit dem Setup fortzufahren, wählen Sie bitte eine dieser aufgeführten Optionen. Wir empfehlen **Deinstallation** für eine saubere Installation. Nach dem Deinstallieren löschen Sie am besten den Ordner `Softwin` aus dem Ordner `Programme`.



3. BitDefender Antivirus v10

Die AntiVirus und AntiSpyware Lösung für Ihren Computer!

BitDefender Antivirus v10 ist eine leistungsstarke AntiVirus und AntiSpyware Software mit den für Sie best möglichen Sicherheitseigenschaften. Durch einfache Anwendung und automatische Updates ist **BitDefender Antivirus** ein Produkt das immer unauffällig im Hintergrund für Sicherheit sorgt.

3.1. Antivirus

Die Aufgabe des Antivirus-Moduls ist sicherzustellen, dass alle Viren entdeckt und beseitigt werden. BitDefender nutzt robuste Scan-Maschinen, die von ICSA Labs, Virus Bulletin, Checkmark, Checkvir und TÜV zertifiziert worden sind.

Pro-aktiver Virenschutz. B-HAVE (Behavioral Heuristic Analyzer in Virtual Environments)ist eine verhaltensbasierte Heuristik-Analyse in virtueller Umgebung und simuliert einen Computer im Computer, in dem Teile der Software auf gefährliches Verhalten überprüft werden. Diese proaktive Technologie stellt eine weitere Sicherheitsebene dar, die das Betriebssystem vor unbekannten Viren schützt, indem gefährliche Kodierungen erkannt werden, für die noch keine Signaturen veröffentlicht wurden.

Permanenter Virenschutz. Die neuen und verbesserten BitDefender-Engines prüfen und desinfizieren infizierte Dateien auf Befehl und minimieren den Datenverlust. Infizierte Dokumente können nun wiederhergestellt werden, anstatt wie früher gelöscht werden zu müssen.

Erkennung und Entfernung von Rootkits. Ein neues BitDefender-Modul überprüft Ihren Computer auf Rootkits (bösartige Softare welche darauf ausgelegt ist verborgen zu bleiben und den Computer fernsteuern kann) und entfernt diese bei Erkennung.

Prüfvorgänge durchführen. Internet Datenverkehr wird in Echtzeit geprüft und bietet ein sicheres und unbeschwertes Surfvergnügen.

Peer-2-Peer Applikationsschutz. Scannt nach Viren, die durch Instant Messaging und Filesharing-Software verteilt werden.

Kompletter E-Mail Schutz. Diese Anwendung funktioniert unter POP3/SMTP Protokollebene und blockiert alle infizierten E-Mail Inhalte, ohne Rücksicht zu nehmen auf den genutzten E-Mail Client (MS Outlook, MS Outlook Express, Netscape, Eudora, Pegasus, The Bat, etc.). Dies geschieht ohne zusätzlichen Konfigurationsaufwand.

3.2. Antispyware

Verhindern Sie, dass Ihr Computer durch Software bedroht ist, die Ihre Daten ausspioniert. Wehren Sie diese Spyware ab, bevor sie Schaden auf Ihrem System anrichtet. Unsere umfangreiche Datenbank hilft Ihnen dabei, Ihren Computer frei von Spyware zu halten. Die BitDefender Spyware Heuristik untersucht eingehende E-Mails nach typischen Spyware-Merkmalen und markiert diese automatisch als Spyware.

Echtzeit-Spywareschutz. BitDefender überwacht Duzende von möglichen Angriffspunkten („HotSpots“) in Ihrem System, die durch Spyware befallen werden könnten. Es überprüft ebenfalls jede Veränderung innerhalb des Systems und der vorhandenen Software. Bekannte Spyware-Programme werden sogar in Echtzeit blockiert.

Überprüfung des Systems. BitDefender kann Ihr System komplett oder teilweise nach Spyware absuchen. Dabei vergleicht das Programm die Merkmale von bekannter Spyware, die in der laufend aktualisierten Softwin Datenbank erfasst sind.

Schutz der Privatsphäre. Der private “Türsteher” überprüft kontinuierlich Internet (http) und Mail (SMTP) Verkehr der Ihren Computer verlässt, ob darin persönliche Daten wir Kreditkartennummer, Kontodaten oder andere Informationen wie z.B. Passwörter enthalten sind sind.

Dialer Schutz. Ein frei konfigurierbarer Dialer-Schutz verhindert, dass Programme ohne Ihr Wissen eine kostenpflichtige Verbindung zum Internet aufbauen können. So sind Sie vor bösen Überraschungen auf Ihrer nächsten Telefonrechnung sicher.

Cookie Kontrolle: Die AntiSpyware filtert eingehende und ausgehende Cookie Dateien, wobei sie die Identität und Einstellungen beim Aufenthalt im Internet vertraulich behandelt.

Kontrolle von aktiven Inhalten: Alle potenziell bösartigen Anwendungen, z. B. ActiveX, Java-Applets oder JavaScript-Code, werden proaktiv blockiert.

3.3. Weitere Eigenschaften

Einsatz und Anwendung. Ein Assistent startet automatisch nach der Installation und hilft den Anwendern die richtigen Einstellungen vorzunehmen, einen Zeitplan festzulegen und stellt einen schnellen Weg zur Registrierung und Aktivierung des Produktes zur Verfügung.

Für den Anwender. BitDefender hat mit Blick auf die Anwenderfreundlichkeit weiter an der Bedieneroberfläche gearbeitet um die einfache Bedienung und die Nutzung zu erleichtern. Als Ergebnis benötigen viele der BitDefender v10 Module deutlich weniger Anwender Interaktion mit Hilfe von bequemer Automatisierung und Lernfähigkeit der Programme.

Stündliche Aktualisierung. Bitdefender aktualisiert sich stündlich über das Internet. Dies geschieht über eine direkte Verbindung oder über einen Proxy-Server. Das Produkt ist darüber hinaus in der Lage sich selbst zu reparieren, indem es defekte oder fehlende Dateien aus dem Internet nachlädt. Besitzer einer BitDefender-Lizenz profitieren auch von kostenlosen Updates und Upgrades auf neuere Versionen.

Kostenloser Support. Werktags steht Ihnen unser deutschsprachiger Support von 8.00 Uhr bis 17.00 Uhr gerne für Fragen zur Verfügung. Unter www.bitdefender.de steht Ihnen unsere Datenbank mit Antworten auf mögliche Fragen rund um die Uhr zur Verfügung. Alle Updates und Produktverbesserungen (Upgrades) sind ab Installationsdatum für einen Zeitraum von 12 Monaten kostenlos. Weitere Informationen finden Sie unter www.bitdefender.de.

Notfall CD. Die **BitDefender Notfall CD** startet Ihren Computer vom CD ROM Laufwerk, falls Windows nicht mehr funktioniert. Danach repariert es mögliche Fehlerquellen und bereinigt Ihren Computer von Viren.



4. BitDefender Module

BitDefender Antivirus v10 beinhaltet die folgenden Module: **Allgemein**, **Antivirus**, **Antispyware** and **Update**.

4.1. Das Modul Allgemein

BitDefender verfügt über eine vollständige Konfiguration für maximale Sicherheit.

Wesentliche Status-Informationen über alle BitDefender-Module werden im Allgemein-Modul angezeigt. Hier können Sie das Produkt registrieren und Grundeinstellungen von BitDefender anpassen.

4.2. Das Modul Antivirus

BitDefender schützt alle gängigen Angriffspunkte auf Ihrem System: E-Mail, Internet-Downloads, Instant Messaging, Netzwerkverbindungen und sämtliche Austauschdatenträger (CD, Diskette, ZIP, USB-Speicher). Vom AntiVirus-Modul aus haben Sie Zugriff auf alle BitDefender-Einstellungen und BitDefender-Eigenschaften.

Der Virenschutz ist in zwei Kategorien aufgeteilt:

- Echtzeit-Virenschutz - verhindert, dass neue Viren Ihr System befallen. Dateien werden gescannt, sobald der Nutzer darauf zugreift. BitDefender zum Beispiel scannt ein Worddokument auf Viren, sobald Sie es öffnen, und E-Mails, sobald Sie sie erhalten. BitDefender prüft Ihre Dateien, sobald Sie sie nutzen.
- Prüfvorgang durchführen - entdeckt residente Viren auf Ihrem System. Das ist der klassische Virenscan, ausgelöst durch den Nutzer – Sie wählen ein Laufwerk einen Ordner oder eine Datei aus und BitDefender scannt sie – nach Aufforderung.

4.3. Das Modul Antispyware

BitDefender überwacht dutzende von möglichen Angriffspunkten (sog. "HotSpots") in Ihrem System, die durch Spyware befallen werden könnten. Es überprüft ebenfalls jede Veränderung innerhalb des Systems und der vorhandenen Software. Bekannte Spyware-Programme werden in Echtzeit blockiert. Die BitDefender AntiSpyware ist höchst effizient in der Bekämpfung von Trojanischen Pferden oder auch anderen bösartigen Instrumenten von Crackern (oftmals als Hacker bezeichnet). Sie bietet einen zuverlässigen Schutz vor Angriffen auf Ihre Privatsphäre und dem unbefugten Versenden persönlicher Daten wie z.B. Kreditkartennummern, PINs oder TANs, usw. von Ihrem Computer zum Angreifer.

4.4. Das Modul Update

Jeden Tag werden neue Viren entdeckt und identifiziert. Aus diesem Grund ist es von großer Bedeutung, dass Sie das Programm BitDefender stets mit den neuesten Virensignaturen betreiben. Standardmäßig prüft BitDefender automatisch im Abstand von drei Stunden, ob neue Updates zur Verfügung stehen.

Folgende Update-Möglichkeiten stehen zur Verfügung:

- **Updates für die Antivirus-Module** - wenn neue Bedrohungen auftreten, müssen die Dateien, in den die Virensignaturen enthalten sind, aktualisiert werden, damit ein kontinuierlicher und aktueller

Schutz auch vor den neuen Gefahren gewährleistet ist. Diese Update-Art wird auch als **Virendefinitions-Update** bezeichnet.

- **Updates für die AntiSpyware Prüfung** - Neue Spyware Signaturen werden kontinuierlich zur BitDefender Datenbank hinzugefügt. Diesen Vorgang nennt man **AntiSpyware-Update**.
- **Produkt-Update** - Wenn eine neue Version von BitDefender erscheint, mit neuen Funktionen und Erkennungstechniken, die eine Verbesserung der Such- und Erkennungsleistung mit sich bringt. Diesen Vorgang nennt man **Produkt-Update**.

Darüber hinaus müssen auch die Update-Arten aufgelistet werden, die einen Benutzereingriff erfordern.

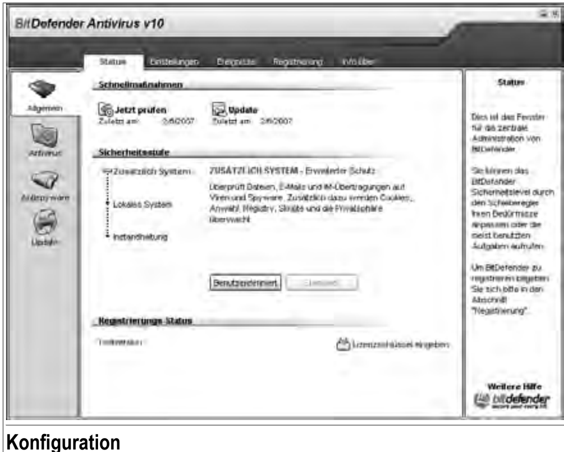
- Automatisches Update - BitDefender verbindet sich automatisch mit dem BitDefender-Update-Server und prüft, ob neue Updates vorhanden sind. Falls entsprechend eingestellt, aktualisiert BitDefender sich automatisch. Das automatische Update kann auch jederzeit über den Klick **Prüfen** gestartet werden.
- Manuelles Update - Download und Installation der neuesten Virendefinitionen erfolgen manuell.



5. Überblick

BitDefender Antivirus v10 enthält eine zentrale Management-Konsole, die es erlaubt, die Schutzfunktionen für alle BitDefender-Module zu konfigurieren. Mit anderen Worten: Es reicht aus, die Management-Konsole zu öffnen, um Zugriff auf alle Module zu haben: **Antivirus**, **Antispyware** and **Update**.

Sie erreichen die BitDefender Management-Konsole über das Windows-Startmenü: **Start** → **Programme** → **BitDefender für File Server** → **BitDefender für File Server**. Schneller geht es jedoch mittels Doppelklick auf das **BitDefender Symbol** in der Systemleiste.



Konfiguration

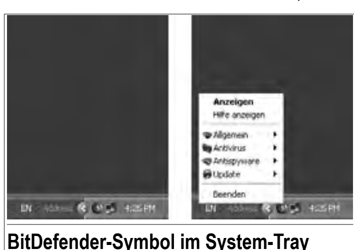
Auf der linken Seite der Management-Konsole sehen Sie die Modulauswahl:

- Allgemein - Sie sehen eine Zusammenfassung aller BitDefender-Einstellungen, überdies Produktdetails und Kontaktinformationen. Hier können Sie auch das Produkt registrieren.
- Antivirus - In diesem Bereich können Sie das **AntiVirus**-Modul konfigurieren.
- AntiSpyware - In diesem Bereich können Sie das **AntiSpyware**-Modul konfigurieren.
- Update - In diesem Bereich können Sie **Updates** konfigurieren.

Im rechten Bereich der Management Konsole sehen Sie Informationen zum jeweiligen Abschnitt, in dem Sie sich befinden. Die Option **Weitere Hilfe**, platziert unten rechts, öffnet die **Online-Hilfe**.

5.1. Systemleiste

Wenn die Konsole minimiert ist, erscheint ein Symbol in der Symbolleiste:



BitDefender-Symbol im System-Tray

Wird das Symbol mit der rechten Maustaste angeklickt, öffnet sich ein Kontextmenü mit folgenden Optionen für die schnelle Verwaltung von BitDefender:

- **Schließen** - minimiert das Programm.
- **Hilfe anzeigen** - öffnet die Hilfe-Datei.
- **Allgemein** - Klicken Sie auf den Button im Modul Allgemein .
  - **Geben Sie den neuen Lizenzschlüssel ein** - Startet den Assistenten, der Sie durch die Registrierung führt.
  - **Erstellen eines Nutzerkontos** - startet den Assistenten, der Ihnen beim Erstellen eines BitDefender Nutzerkontos hilft.
- **BitDefender AntiVirus** - klicken Sie auf diesen Button, um das AntiVirus Modul zu öffnen.
  - **Echtzeitschutz aktiviert/deaktiviert** - Zeigt den Status des Echtzeitschutzes an(aktiviert/deaktiviert). Klicken Sie diesen Button um den Echtzeitschutz zu aktivieren/deaktivieren.
  - **Durchsuchen** - öffnet ein Fenster, in welchem Sie die Berichtsdateien, die Sie sich ansehen wollen, auswählen können.
- **BitDefender AntiSpyware** - klicken Sie auf diesen Button, um das AntiSpyware Modul zu öffnen.
  - **Verhaltensbasierte Antispyware ist aktiviert/deaktiviert** - Zeigt den Status des Echtzeit AntiSpyware Schutzes an (aktiviert/ deaktiviert). Klicken Sie hier um den Echtzeit AntiSpyware Schutz zu aktivieren/deaktivieren.
  - **Erweiterte Einstellungen** - Möglichkeit die AntiSpyware Kontrolle zu konfigurieren.
- **Update** - klicken Sie auf diesen Button, um die Option Update zu öffnen.
  - **Update jetzt durchführen** - führt unverzüglich ein verfügbares Update von BitDefender durch.
  - **Automatisches Update ist aktiviert/ deaktiviert** - zeigt den Status des Automatischen update (aktiviert/deaktiviert). Klicken Sie hier um das Automatische Update zu aktivieren/deaktivieren.
- **Beenden** - beendet die Anwendung. Bei der Auswahl dieser Option verschwindet das Symbol von der Symbolleiste. Für einen erneuten Zugriff starten Sie aus dem Start-Menü.



Anmerkung

Wenn Sie ein oder mehrere Module von BitDefender deaktivieren verändert sich das Symbol von BitDefender in der System-Tray. So werden Sie auch bei geschlossener Konsole über den Status von BitDefender informiert.
Das BitDefender-Symbol blinkt wenn ein Update zur Verfügung steht.



5.2. Aktivitsänzeige

Die **Aktivitätsanzeige** ist eine graphische Visualisierung der Prüfaktivität auf Ihrem System.



Aktivitäsanzeige

Die grünen Balken (die **Datei-Zone**) zeigen die Anzahl der gescannten Dateien pro Sekunde, auf einer Skala von 0 bis 50.



Anmerkung

Die **Aktivitätsanzeige** informiert Sie mit einem roten „X“, wenn das Virus Schild deaktiviert ist (**Datei**). Somit sind Sie über diesen Zustand auch informiert, wenn die Management Konsole nicht geöffnet ist.

Wenn Sie die graphische Visualisierung nicht länger sehen wollen, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Ausblenden**.



Anmerkung

Um das Fenster komplett zu verbergen, entfernen Sie das Häkchen bei **Aktivitätsanzeige einblenden** (im Abschnitt Einstellungen im Menüpunkt **Allgemein**).



6. Das Modul Allgemein

Der Abschnitt **Allgemein** behandelt und erklärt folgende Themen:

- Status aller BitDefender Module
- Allgemeine Einstellungen
- Ereignisanzeige
- Registrierung des Produkts
- Info über




Weitere Inhalte und Einzelheiten zum Modul **Allgemein** finden Sie in der Produktbeschreibung auf Seite „*Das Modul Allgemein*“ (S. 15).

6.1. Status aller BitDefender Module

Um diese Sektion zu öffnen klicken Sie bitte auf **Status** im Modul **Allgemein**.



Status aller BitDefender Module

In diesem Abschnitt können Sie alle wichtigen Sicherheitseinstellungen von BitDefender vornehmen. Hier können Sie das Produkt registrieren und das Ablaufdatum ablesen.

6.1.1. Schnell Einstellungen

BitDefender erlaubt schnellen Zugang zu allen Sicherheitseinstellungen. Mit Hilfe dieser Einstellungen bleibt BitDefender aktuell, Sie können das System prüfen oder Datenverkehr blockieren.

Um das gesamte System zu prüfen klicken Sie einfach **Jetzt scannen** - Das Prüffenster erscheint Prüffenster und die Systemprüfung wird gestartet.



Wichtig

Wir empfehlen dringend, einen kompletten Virenscan mindestens einmal in der Woche durchzuführen. Um einen kompletten Systemscan durchzuführen, aktivieren Sie das **AntiVirus**-Modul, Sektion Prüfen, wählen Sie die zu prüfenden **Lokalen Laufwerke** aus und klicken Sie dann auf **Prüfen**.

Bevor Sie die Systemprüfung starten, empfehlen wir Ihnen BitDefender zu aktualisieren. So können auch die neuesten Schädlinge entdeckt werden. Um BitDefener zu aktualisieren klicken Sie **Update**. Warten Sie bis der Update Prozess abgeschlossen ist. Sie könne auch unter Update den Update Status verfolgen.



Anmerkung

Weitere Informationen über den Update Prozess finden Sie im Kapitel Update in diesem Handbuch.

6.1.2. Sicherheitseinstellungen

Sie könnnen die Einstellungen so vornehmen, wie Sie Ihren Sicherheitsanforderungen am besten entsprechen. Ziehen Sie den Zeiger auf der Scala entlang, um Ihr Sicherheitslevel einzustellen.

Es gibt 3 mögliche Einstellungen:

Sicherheitseinstellungen	Beschreibung
Wartung	Bietet keinen Schutz. Es ist nur das **Automatische Update** aktiviert. BitDefender wird nur aktualisiert. Auch wenn kein Schutz geboten wird, könnte diese Einstellung für System Administratoren nützlich sein.
Lokales Verzeichnis	Bietet Virenschutz. Empfohlen für Computer ohne Netzwerk oder Internet Verbindung. Geringe Belastung der Ressourcen. Prüft alle vorhanden Dateien.
Lokales System	Bietet Schutz vor Viren und Spyware. Speziell empfohlen für Computer ohne Netzwerk oder Internet Anschluss. Geringe Belastung der Ressourcen. Prüft alle vorhanden Dateien.

BitDefender Antivirus v10 wird empfohlen für Computer ohne Netzwerk oder Internet Anschluss.

Sie können das Sicherheitslevel ändern, indem Sie auf **Benutzerdefiniert** klicken. Im neuen Fenster das nun erscheint können Sie die gewünschten Schutzmaßnahmen auswählen. Klicken Sie zum Bestätigen auf **OK**.

Mit dem Klick auf **Standard** laden Sie die Grundeinstellungen.

6.1.3. Status der Registrierung

Dieser Abschnitt enthält Informationen zum Status Ihrer BitDefender Lizenz. Hier können Sie das Produkt registrieren und das Ablaufdatum ablesen.

Um einen neuen Lizenzschlüssel einzugeben klicken Sie **Neuen Lizenzschlüssel eingeben**. Beenden Registrierungs Assistent um BitDefender erfolgreich zu registrieren.



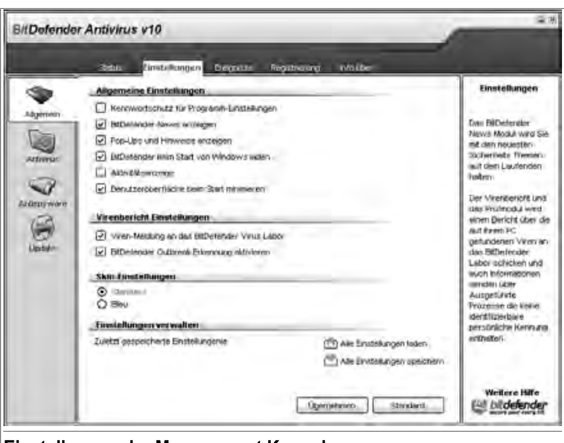
Anmerkung

Weitere Informationen über die Registrierung finden Sie im Kapitel Produkt Registrierungin diesem Handbuch.



6.2. Einstellungen der Management Konsole

Um diese Sektion zu öffnen klicken Sie bitte auf **Einstellungen** im Modul **Allgemein**.



Einstellungen der Management Konsole

Hier können Sie die umfassenden Einstellungen von BitDefender einsehen. Standardmäßig wird BitDefender beim Windowsstart geladen und läuft dann im Hintergrund.

Sie können zwischen 4 Kategorien auswählen: **Allgemeine Einstellungen**, **Einstellung Viren Report** , **Einfache Einstellung** und **Einstellungen verwalten**.

6.2.1. Allgemeine Einstellungen

- **Konsole per Kennwort schützen** - die Passwort-Einstellung aktivieren, um Ihre BitDefender-Einstellungen zu schützen.



Anmerkung

Wenn Sie nicht der einzige Benutzer des Computers sind, empfehlen wir Ihnen, Ihre vorgenommenen Einstellungen mit einem Passwort zu schützen.

Wenn Sie diese Option wählen erscheint das folgende Fenster:



Kennwort bestätigen

Schreiben Sie ein Passwort in das **Kennwort**-Feld und wiederholen Sie es in dem Feld **Wiederholung**. Danach klicken Sie auf **OK**.

Von nun an werden Sie stets aufgefordert, Ihr Passwort einzugeben, wenn Sie die Einstellungen von BitDefender ändern wollen.



Wichtig

Falls Sie Ihr Passwort vergessen haben sollten, müssen Sie unter Reparieren Ihre BitDefender-Konfiguration modifizieren.

- **Sicherheits-Mitteilungen anzeigen** - von Zeit zu Zeit empfangen Sie Sicherheitsmeldungen, die von BitDefender-Servern versendet werden.
- **Hinweise anzeigen** - Pop-up-Fenster anzeigen, die über den Produktstatus informieren.
- **BitDefender beim Start von Windows laden** - automatisches Starten des BitDefenders beim Systemstart.



Anmerkung

Dies wird dringend empfohlen.

- **Prüfanzeige aktivieren (Grafische Anzeige Produkt Aktivität)** - (de)aktiviert auf Wunsch den Prüfanzeige von BitDefender.
- **Minimiert starten** - minimiert die BitDefender-Management-Konsole, nachdem das System gestartet worden ist. Nur das BitDefender Symbol erscheint in der Systemablage.

6.2.2. Einstellung Virenbericht

- **Viren-Meldung an das BitDefender Virus Labor** - sendet erkannte Viren an das BitDefender-Virenlabor. Diese Meldung zeigt uns die Verbreitung von Viren an und hilft uns, geeignete Gegenmaßnahmen ergreifen zu können.

  Der Report enthält keinerlei vertrauliche Daten, wie z. B. Ihren Namen oder Ihre IP-Adresse, und wird nicht für kommerzielle Zwecke verwendet. Die gelieferten Informationen enthalten den Virennamen und werden lediglich für statistische Zwecke benötigt.
- **Viren-Meldung an das BitDefender Virus Labor** - sendet erkannte Viren an das BitDefender-Virenlabor. Diese Meldung zeigt uns die Verbreitung von Viren an und hilft uns, geeignete Gegenmaßnahmen ergreifen zu können.

  Der Report enthält keinerlei vertrauliche Daten, wie z. B. Ihren Namen oder Ihre IP-Adresse, und wird nicht für kommerzielle Zwecke verwendet. Die gelieferten Informationen enthalten den Virennamen und werden lediglich für statistische Zwecke benötigt.

6.2.3. Auswahlfenster Einstellungen

Oberflächen - Datei erlaubt Ihnen, die Farbe der Management-Konsole zu wählen. Der Skin repräsentiert die Hintergrundgrafiken und Symbolfarben in der Benutzeroberfläche. Klicken Sie auf die jeweilige Bezeichnung, um die Benutzeroberfläche gemäß Ihren Wünschen anzupassen.

6.2.4. Update-Einstellungen

Verwenden Sie die Option **Alle Einstellungen speichern** / **Alle Einstellungen laden** um eine Sicherungskopie sämtlicher in BitDefender vorgenommenen Einstellungen zu exportieren und nach einer Reparatur wieder zu importieren.



Wichtig

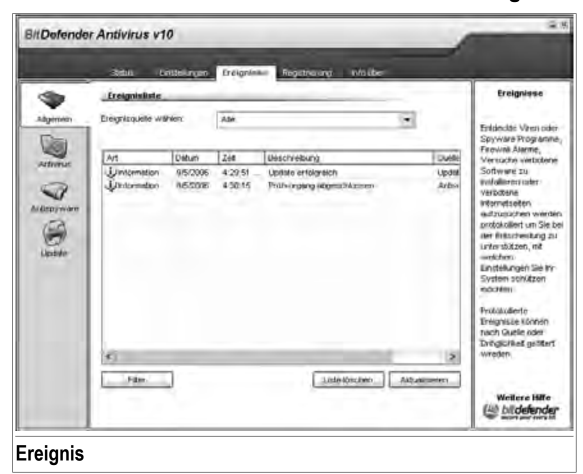
Nur Anwender mit Administratoren Rechten können die Einstellungen ändern.



Klicken Sie auf **Übernehmen** um die Einstellungen zu speichern. Wenn Sie auf **Standard** klicken, werden die Werkseinstellungen geladen.

6.3. Ereignis

Um diese Sektion zu öffnen klicken Sie bitte auf **Ereignisse** im Modul **Allgemein**.



Ereignis

In dieser Sektion sind sämtliche von BitDefender erstellten Ereignisse angezeigt.

Es gibt drei Arten von Ereignissen: **Information**, **Warnung** und **Kritisch**.

Beispiel für solche Ereignisse:

- **Information** - Wenn eine E-Mail überprüft wurde;
- **Warnung** - Wenn eine verdächtige Datei gefunden wurde;
- **Kritisch** - Wenn eine infizierte Datei gefunden wurde.

Für jedes Ereignis werden die folgenden Informationen bereitgestellt: Datum und Uhrzeit, zu der das jeweilige Ereignis stattgefunden hat, eine kurze Beschreibung und seine Quelle (**AntiVirus** oder **Update**). Klicken Sie doppelt auf ein bestimmtes Ereignis und Sie erhalten weitere Informationen zu diesem.

Es ist möglich, die angezeigten Ereignisse auf zwei Arten zu filtern – nach Quelle oder nach Art:

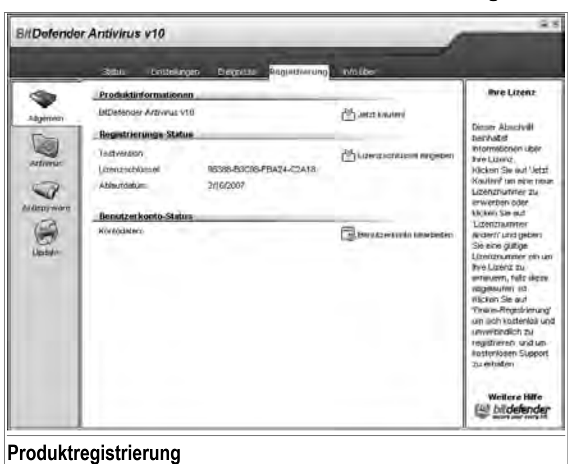
- Klicken Sie auf **Filter** und wählen Sie die gewünschte Ereignisart aus;
- Wählen Sie die Ereignisquelle, aus der gleichnamigen Dropdownliste.

Ist die Sektion **Ereignisse** bereits geöffnet, so müssen Sie auf die Schaltfläche **Aktualisieren**klicken, um neu hinzu gekommene Ereignisse anzeigen zu lassen.

Um alle Ereignisse zu löschen, klicken Sie bitte auf die Schaltfläche **Liste löschen**.

6.4. Produktregistrierung

Um diese Sektion zu öffnen klicken Sie bitte auf **Registrieren** im Modul **Allgemein**.



Produktregistrierung

Dieser Abschnitt enthält Informationen zum Produkt BitDefender (Status der Registrierung, Produkt ID, Ablaufdatum der Lizenz). Hier können Sie das Produkt registrieren und Ihr BitDefender Nutzerkonto konfigurieren.

Klicken Sie **Jetzt kaufen** um eine neue BitDefender Lizenz online zu kaufen.

Klicken Sie **Neuen Lizenzschlüsssel eingeben** Sie können das Produkt registrieren, die Registrierung oder Ihre Nutzerdaten ändern. Um Ihr Nutzerkonto zu konfigurieren klicken Sie **Nutzerkonto konfigurieren**. In beiden Fällen erscheint der Registrierungsassistent.



6.4.1. Konfigurations-Assistent

Der Konfigurations-Assistent besteht aus 5 einzelnen Schritten.

Schritt 1/5 - Willkommen beim BitDefender Konfigurations-Assistent.



Begrüßungsfenster

Klicken Sie auf **Weiter**.

Schritt 2/5 Wie kann ich BitDefender registrieren?



Registrierung

Wählen Sie **Produkt registrieren** um **BitDefender Antivirus v10** zu registrieren. Geben Sie im Feld **neuen Lizenzschlüssel eingeben** den Lizenzschlüssel ein.

Um das Produkt weiter zu testen, klicken Sie bitte auf die Schaltfläche **Produkt weiter testen**.

Klicken Sie auf **Weiter**.

Schritt 3/5 – Einrichten eines BitDefender Nutzerkontos.



Kontoerstellung

Ich habe noch kein BitDefender Benutzerkonto

Um vom technischen Support von BitDefender zu profitieren und weitere zur Verfügung stehende Services zu erhalten müssen Sie ein Nutzerkonto einrichten.

Tragen Sie eine gültige E-Mail Adresse **E-mail** in das Feld ein. Legen Sie ein Passwort fest und geben es in das Feld **Password** ein. Bestätigen Sie das Passwort **durch Wiederholen** . Zum Einloggen in Ihr Nutzerkonto benutzen Sie Ihre E-Mail und das Passwort http://myaccount.bitdefender.com.



Anmerkung

Das Passwort sollte mindestens 4 Zeichen haben.

Um erfolgreich ein Nutzerkonto einzurichten müsssen Sie zunächste Ihre E-Mail Adresse aktivieren. Überprüfen Sie Ihre E-Mail Adresse und folgen Sie den Instruktionen, die Ihnen per E-Mail vom BitDefender Registrierungsservice zugeschickt wurden.



Wichtig

Bitte aktivieren Sie Ihr Nutzerkonto bevor Sie zum nächsten Schritt weitergehen.

Wenn Sie kein BitDefender Nutzerkonto einrichten wollen, klicken Sie auf **Diesen Schritt überspringen**. Überspringen Sie ebenfalls den nächsten Schritt des Assistenten.

Klicken Sie auf **Weiter**.

Ich habe bereits ein BitDefender Nutzerkonto.

Wenn Sie bereits ein aktives Nutzerkonto haben, geben Sie Ihre E-Mail und das Passwort ein. Wenn Sie ein falsches Passwort eingeben, werden Sie zur Wiederholung aufgefordert, wenn Sie auf **Weiter** klicken. Klicken Sie **Ok** um das Passwort nochmal einzugeben oder **abbrechen** um den Assistenten zu beenden.

Wenn Sie Ihr Passwort vergessen haben, klicken Sie **Passwort vergessen?** und folgen Sie den Instruktionen.

Klicken Sie auf **Weiter**.



Schritt 4/5 - Auswählen der Prüfoptionen



Daten Nutzerkonto



Anmerkung
Dieser Schritt wird ausgelassen, wenn Sie auf **Schritt auslassen** klicken im Schritt 3.

Tragen Sie Ihren Vor- und Nachnahmen ein und wählen Sie ein Land aus.

Wenn Sie bereits ein BitDefender Nutzerkonto eingerichtet haben, wird der Assistent Ihnen die vorhandenen Informationen anzeigen. Sie können diese Informationen ändern.



Wichtig
Die hier eingetragenen Daten bleiben vertraulich.

Klicken Sie auf **Weiter**.

Schritt 5/5 – Übersicht



Fertigstellen

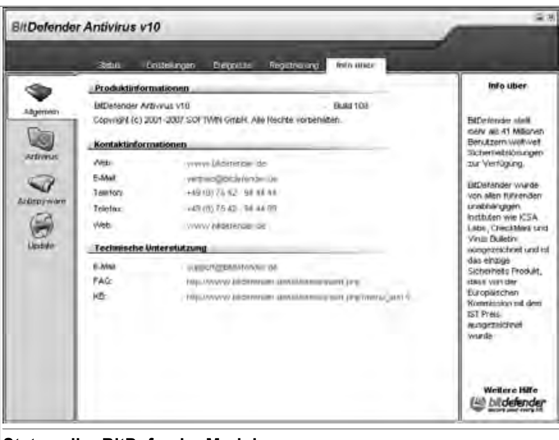
Dies ist der letzte Schritt der Konfigurationsassistenten. Sie können jedoch jegliche Veränderungen vornehmen, in dem Sie zu den vorherigen Schritten zurückkehren (Klicken Sie auf **Zurück**).

Wenn Sie keine Änderungen vornehmen wollen klicken Sie bitte auf **Fertigstellen**.

Klicken Sie in der BitDefender Management-Konsole auf die Option **Berichte**

6.5. Info

Um diese Sektion zu öffnen klicken Sie bitte auf **Info über** im Modul **Allgemein**.



Status aller BitDefender Module

Hier finden Sie eine Übersicht über den Produkt-Status und Kontakt Informationen.

BitDefender stellt Sicherheitslösungen bereit, die den heutigen Anforderungen an sichere Computersysteme gerecht werden. Mit über 41 Millionen Privat- und Unternehmenskunden in mehr als 100 verschiedenen Ländern ist BitDefender eine der meist genutzten Sicherheitslösungen weltweit.

Die Scan-Engine von BitDefender™ist von unabhängigen Instituten wie z.B. - **ICSA Labs**, **CheckMark** und **Virus Bulletin** zertifiziert. BitDefender ist überdies das einzige Sicherheitsprodukt, das eine Auszeichnung (**IST-Prize**) von der Europäischen Kommission erhalten hat.

Weitere Informationen über BitDefender erhalten Sie unter:www.bitdefender.de



7. Das Modul Antivirus

Der Abschnitt **AntiVirus** behandelt und erklärt folgende Themen:

- Bei Zugriff scannen
- Nach Aufforderung prüfen
- Quarantäne

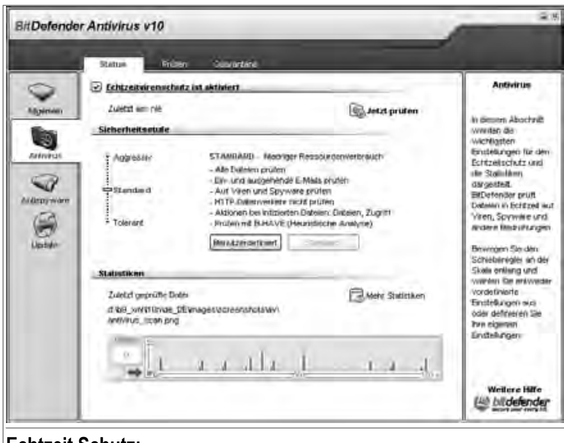


Anmerkung

Weitere Inhalte und Einzelheiten zum Modul **AntiVirus** finden Sie in der Produktbeschreibung auf Seite „*Das Modul Antivirus*“ (S. 15).

7.1. On-Access-Scannen

Um diese Sektion zu öffnen klicken Sie bitte auf **Schild** im Modul **Antivirus**.



Echtzeit Schutz:

In diesem Abschnitt können Sie das **Virus Schild** konfigurieren und Informationen über dessen Aktivität einsehen. Das **Virus Schild** schützt alle gängigen Einstiegspunkte auf Ihrem System: E-Mail, Internet- Downloads, Instant Messaging, Netzwerkverbindungen und sämtliche Austauschdatenträger (CD, Diskette, ZIP-Laufwerke, USB-Speicher).



Wichtig

Um zu verhindern, dass Viren Ihren Computer befallen, lassen Sie das **Virus Schild** immer aktiviert.

Am unteren Ende dieser Registerkarte sehen Sie die **Virus Schild**-Statistik über Dateien und E-Mail-Nachrichten. Klicken Sie auf **Mehr Statistiken**, wenn Sie mehr Informationen erhalten wollen.

7.1.1. Sicherheitseinstellung

Sie können die Sicherheitseinstellung an Ihre Anforderungen anpassen. Ziehen Sie die Anzeige auf der Scala auf die richtige Einstellung.

Es gibt 3 mögliche Einstellungen:

Sicherheitseinstellung	Beschreibung
Zulassen	Deckt einfache Anforderungen ab. Geringe Belastung der Ressourcen. Programme und eingehende Nachrichten werden nur auf Viren hin geprüft. Neben den klassischen Signatur basierten Scans werden außerdem Heuristische Scans eingesetzt. Bei infizierten Dateien können Sie wählen zwischen Datei bereinigen/Zugriff verweigern.
Standardeinstellung	Gewährleistet Standard Sicherheit. Belsatung der Ressourcen ist gering. Alle eingehenden und ausgehenden Nachrichten werden auf Viren und Spyware geprüft. Sowohl mit Hilfe des klassischen Scans als auch der Heuristik. Bie infizierten Dateinen können Sie wählen zwischen Datei bereinigen/Zugriff verweigern.
Aggressiv	Gewährleistet hohe Sicherheit. Mittlere Belastung der Ressourcen. Alle eingehenden und ausgehenden Nachrichten werden auf Viren und Spyware geprüft. Sowohl mit Hilfe des klassischen Scans als auch der Heuristik. Bie infizierten Dateinen können Sie wählen zwischen Datei bereinigen/Zugriff verweigern.

Benutzer mit Vorkenntnissen sollten sich die Prüfeinstellungen von BitDefender genauer ansehen. Bestimmte Dateierweiterungen, Verzeichnisse und Archive, die wahrscheinlich keine Bedrohung darstellen, können vom Scan ausgeschlossen werden. So wird die Prüfzeit verringert und das Reaktionsvermögen Ihres Rechners während eines Scans verbessert.

Sie können das Level für den gewünschten Schutz einstellen. Klicken Sie **Level anpassen**. Das folgende Fenster öffnet sich:



Einstellungen des Virus Schild

Die Prüfeinstellungen sind wie ein aufklappbares Windows-Explorermenü aufgebaut.

Klicken Sie auf "+", um eine Option zu öffnen, und auf "-", um diese zu schließen.

Sie können sehen, dass sich einige Prüfoptionen nicht öffnen lassen, obwohl das "+"- Zeichen sichtbar ist. Der Grund dafür ist, dass diese Optionen bisher nicht gewählt worden sind. Wenn Sie diese Optionen auswählen, können sie geöffnet werden.



- **Dateizugriffe und P2P-Übertragungen prüfen** - um alle Dateien und die Kommunikation mit Instant Messengers (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) zu überprüfen. Des Weiteren wählen Sie eine Datei aus, die Sie prüfen möchten.

Option		Beschreibung
Dateien prüfen	**Alle Dateien prüfen**	Prüft alle vorhanden Dateien.
	Programmdateien	Prüft ausschließlich Dateien mit den Dateiendungen: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml und .nws.
	Nur Dateien mit folgenden Erweiterungen	Nur die Dateien werden überprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.
	Erweiterungen ausschließen	Nur die Dateien werden NICHT geprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.
	Auf Spyware prüfen	Sucht nach möglichen Spyware-Anwendungen. Entsprechende Riskware-Dateien werden wie infizierte Dateien behandelt. Software mit Adware-Komponenten arbeitet unter Umständen nicht mehr, wenn diese Option aktiviert ist. Wählen Sie **Dialer und Anwendungen vom Scan ausschließen**, wenn Sie diese Dateien vom Scan ausschließen wollen.
Arbeitsspeicher prüfen		Scanned das CD Laufwerk auf Zugriff.
Archive prüfen		Auch der Inhalt von Archiven wird geprüft. Ist diese Option aktiviert, so kann es zur Verlangsamung des Computers führen.
Komprimierte Dateien prüfen		Alle komprimierten Dateien werden überprüft.
Direktverbindung		Nun können Sie eine der folgenden Möglichkeiten auswählen:
	Zugriff verhindern und fortfahren	Im Falle eines Virenfundes wird der Zugriff auf die Datei verhindert.
	Datei säubern	Um die infizierte Datei zu desinfizieren.
	Datei löschen	Die infizierte Datei wird ohne Warnung sofort gelöscht.
	In Quarantäne verschieben	Die infizierte Datei wird in die Quarantäne verschoben.
Aktionsoptionen		**Zweite Aktion, falls die erste fehlschlägt** - Wählen Sie hier eine Aktion, die ausgeführt werden soll, wenn die erste Aktion fehlschlägt.
	Zugriff verhindern und fortfahren	Im Falle eines Virenfundes wird der Zugriff auf die Datei verhindert.
	Datei löschen	Die infizierte Datei wird ohne Warnung sofort gelöscht.

Option		Beschreibung
	In Quarantäne verschieben	Die infizierte Datei wird in die Quarantäne verschoben.
Dateien größer als (x) nicht prüfen		**Dateien größer als [x] nicht prüfen** - geben Sie die maximale Größe der zu prüfenden Datei ein. Falls die Größe 0 Kb ist, werden alle Dateien geprüft.
Erweiterungen ausschließen		**Pfade nicht prüfen** - Klicken Sie auf "+" um einen Ordner auszuwählen, der nicht geprüft werden soll. Die Konsequenz ist, dass die Option ausgeweitet wird und `Neues Objekt` erscheint. Klicken Sie auf die dazu gehörende Box und wählen Sie aus dem Fenster die Datei aus, die nicht geprüft werden soll. Die hier ausgewählten Objekte werden vom Scan ausgeschlossen, unabhängig vom festgelegten Schutz Level. (nur für **Anpassen Level**).

- **E-Mails prüfen** - prüft alle E-Mail-Nachrichten.

  Folgende Optionen stehen zur Verfügung:

Option	Beschreibung
Eingehende E-Mails prüfen	Prüft alle eingehenden E-Mails und deren Attachments.
Ausgehende E-Mails prüfen	Prüft alle ausgehenden E-Mails.

- **HTTP Datenverkehr prüfen** - prüft HTTP Datenverkehr.
- **Warnen wenn ein Virus entdeckt wurde** - zeigt eine Warnmeldung an, wenn ein Virus in einer Datei oder E-Mail gefunden wurde.

  Ist eine Datei infiziert wird eine Warnmeldung ausgegeben, die Hinweise über die Art des Schädlings beinhaltet. Bei infizierten E-Mails erhält der Empfänger eine Nachricht mit Hinweisen über die Art des Schädlings und Informationen über den Absender der Nachricht.

  Im Falle eines Verdachts kann ein Assistent aufgerufen werden der Ihnen dabei hilft, verdächtige Dateien zur weiteren Analyse an das BitDefender Virus Labor zu senden. Optional können Sie Ihre E-Mail-Adresse angeben, um weitere Informationen zur Analyse zu erhalten.

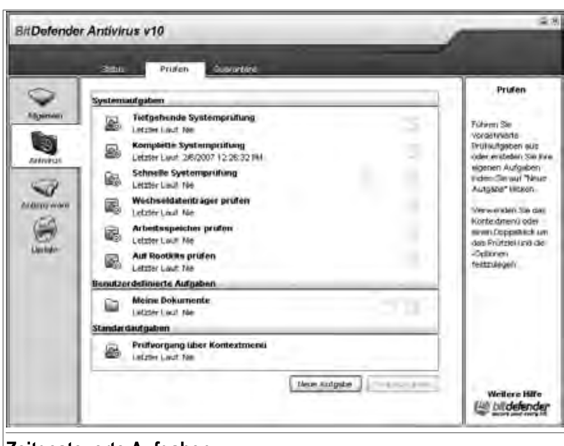
Klicken Sie auf **OK**, um die Änderungen zu speichern.

Wenn Sie zu den Standardeinstellungen zurückkehren wollen, klicken Sie auf **Standardeinstellung**.



7.2. On-Demand-Scannen

Um diese Sektion zu öffnen klicken Sie bitte auf **Prüfen** im Modul **Antivirus**.



Zeitgesteuerte Aufgaben

In diesem Fenster können Sie die BitDefender Einstellungen zur Prüfung Ihres Computers vornehmen.

Die Aufgabe der BitDefender-Software ist es sicherzustellen, dass es keine Viren in Ihrem System gibt. Dies wird in erster Linie erreicht, indem Ihre E-Mail-Anhänge und Downloads überprüft und alle Aktionen, die auf Ihrem System stattfinden, überwacht werden.

Es besteht aber die Gefahr, dass ein Virus bereits in Ihrem System ist, bevor Sie BitDefender installieren. Deshalb sollten Sie Ihren Computer nach der Installation von BitDefender auf residente Viren prüfen. Übrigens sollten Sie Ihren Computer auch in Zukunft häufig auf Viren prüfen.

7.2.1. Zeitgesteuerte Aufgaben

Der On-Demand Scan richtet sich nach den Prüfoptionen. Der Anwender kann mit Hilfe der Standardeinstellungen oder eigenen Prüfoptionen den Scan durchführen.

Es gibt drei verschiedene Einstellungen der Prüfoptionen:

- **Systemaufgaben** - Enthält eine Liste von standard Systemeinstellungen. Die folgenen Einstellungen sind möglich:

Standard Einstellungen	Beschreibung
Tiefgehende Systemprüfung	Prüft alle vorhandenen Dateien auf Viren und Spyware.
Prüfen des gesamten Systems	Prüft alle vorhandenen Dateien mit Ausnahme von Archiven auf Viren und Spyware.
Schnelle Systemprüfung	Prüft alle Programmdateien auf Viren und Spyware.
Prüfen von Wechsellaufwerken	Prüft Wechsellaufwerke auf Viren und Spyware.

Standard Einstellungen	Beschreibung
Arbeitsspeicher überprüfen	Überprüft den Arbeitsspeicher auf bekannte Malware.
Auf Rootkits prüfen	Prüft Speicher auf getarnte Malware.

- **Benutzerdefinierte Aufgaben** - enthält die Anwender definierten Tasks.

  Prüfoption `Meine Dokumente`. Nutzen Sie diese Prüfoption, um Ihre Dokumente im Verzeichnis `Meine Dokumente` zu prüfen.
- **Standardaufgaben** - enthält eine Liste verschiedener Prüfoptionen. Diese Optionen weisen auf andere Prüfoptionen hin, die in diesem Fenster nicht ausgeführt werden können. Sie können nur die Einstellungen ändern oder die Prüfberichte ansehen.

Drei Schaltflächen sind verfügbar:

- **Tasks planen** - zeigt an, dass die ausgewählte Aufgabe für später geplant ist. Klicken Sie **Geplante Tasks** - zeigt an, dass die ausgewählte Task zu einem späteren Zeitpunkt geplant ist. Klicken Sie auf Planer im Abschnitt **Eigenschaften** In diesem Fenster können Sie die Einstellungen ändern.
- **Löschen** - löscht die ausgewählte Aufgabe.



Anmerkung

Für Systemaufgaben nicht verfügbar. Sie können Systemaufgaben nicht löschen.

- **Jetzt prüfen** - führt die ausgewählte Aufgabe aus, indem ein immediate scan durchgeführt wird.

7.2.2. Eigenschaften der Prüfoptionen.

Jede Prüfung hat ihre eigenen **Eigenschaften** ein Fenster indem Sie die prüfoptionen konfigurieren können, das Ziel der Prüfung festlegen,die Tasks planen oder die Berichte ansehen. Öffnen Sie das Fenster mit einem Doppelklick. Das folgende Fenster erscheint:



Auswahlfenster Einstellungen



Auswahlfenster Einstellungen

Hier finden Sie Informationen über Aufgaben (Name, letzte Prüfung und geplante Tasks) und können die Prüfeinstellungen setzen.

Prüflevel

Sie müssen zunächst das Level der Prüfung einstellen. Ziehen Sie dazu den Zeiger an der Skala entlang, bis Sie das gewünschte Level erreicht haben.

Es gibt 3 mögliche Einstellungen:

Sicherheitseinstellung	Beschreibung
Niedrig	Bietet ausreichende Entdeckung. Belastung der Ressourcen ist niedrig. Die Programme werden nur auf Viren hin geprüft. Neben der Signatur-basierten Prüfung wird ebenfalls die Heuristik eingesetzt. Sie können im Falle von infizierten Dateien wählen: Datei reparieren/in Quarantäne verschieben.
Mittel	Bietet eine gute Entdeckung. Belastung der Ressourcen ist mittel. Alle Dateien werden auf Viren und Spyware geprüft. Neben der Signatur-basierten Prüfung wird ebenfalls die Heuristik eingesetzt. Sie können im Falle von infizierten Dateien wählen: Datei reparieren/in Quarantäne verschieben.
Hoch	Bietet eine hohe Entdeckung. Belastung der Ressourcen ist hoch. Alle Dateien und Archive werden auf Viren und Spyware geprüft. Neben der Signatur-basierten Prüfung wird ebenfalls die Heuristik eingesetzt. Sie können im Falle von infizierten Dateien wählen: Datei reparieren/in Quarantäne verschieben.



Wichtig

Auf Rootkits prüfen beinhaltet dieselbe Prüftiefe, jedoch gibt es unterschiedliche Optionen:

- **Niedrig** - Es werden nur Prozesse überprüft und bei Erkennung wird keine Aktion durchgeführt.

- **Mittel** - Dateien und Prozesse werden überprüft, es wird nach versteckten Objekten gesucht und bei Erkennung wird keine Aktion durchgeführt.
- **Hoch** - Dateien und Prozesse werden überprüft, es wird nach versteckten Objekten gesucht und bei Erkennung werden diese umbenannt.

Benutzer mit Vorkenntnissen sollten sich die Prüfeinstellungen von BitDefender genauer ansehen. Bestimmte Dateierweiterungen, Verzeichnisse und Archive, die wahrscheinlich keine Bedrohung darstellen, können vom Scan ausgeschlossen werden. So wird die Prüfzeit verringert und das Reaktionsvermögen Ihres Rechners während eines Scans verbessert.

Anpassen - um Ihre eigenen Prüfoptionen zu setzen. Das folgende Fenster öffnet sich:



Auswahlfenster Einstellungen

Die Prüfeinstellungen sind wie ein aufklappbares Windows-Explorermenü aufgebaut.

Die Prüfoptionen sind in fünf Kategorien unterteilt:

- **Virus Prüfoptionen**
- **Spyware Prüfoptionen**
- **Aktionsoptionen**
- **Berichtoptionen**
- **Weitere Optionen**

Klicken Sie auf "+", um eine Option zu öffnen, und auf "-", um diese zu schließen.



Wichtig

Für den **Auf Rootkits prüfen** Task sind drei Kategorien verfügbar: **Rootkit Prüfoptionen**, **Berichtsoptionen** und **Weitere Optionen**. In der ersten Kategorie können Sie wählen was geprüft werden soll (Dateien, Arbeitsspeicher, oder beides) und welche Aktion bei Erkennung durchgeführt werden soll (Keine (nur protokollieren) oder Umbenennen). Die letzten beiden Kategroien sind identisch mit den unten beschriebenen.

- Geben Sie an, welche Arten von Objekte geprüft werden sollen (Archiv, Postfächer, etc.). Weitere Optionen können über die Kategorie **Virus Prüfoptionen** angegeben werden.



Option		Beschreibung
Dateien prüfen	**Alle Dateien prüfen**	Prüft alle vorhanden Dateien.
	Programmdateien	Prüft ausschließlich Dateien mit den Dateiendungen: exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml und nws.
	Nur Dateien mit folgenden Erweiterungen	Nur die Dateien werden überprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.
	Folgende Erweiterungen ausschließen	Nur die Dateien werden NICHT geprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.
Boot-Sektoren prüfen		Prüft die Bootsektoren des Systems.
Speicher prüfen		Prüft den Speicher auf Viren und andere Malware.
Auf Riskware prüfen		Sucht neben Viren ebenfalls nach anderen Bedrohungen wie Dialern und Adware. Entsprechende Riskware-Dateien werden wie infizierte Dateien behandelt. Software mit Adware-Komponenten arbeitet unter Umständen nicht mehr, wenn diese Option aktiviert ist. Wählen Sie **Anwendungen und Dialer ausschließen**, wenn Sie diese Dateien von der Prüfung ausschließen wollen.
Erweiterte Prüfoptionen	**Komprimierte Dateien**	Alle komprimierten Dateien werden überprüft.
	Archive	Prüft den Inhalt von eingepackten Archiven.
	Postfächer	Prüft den Inhalt von E-Mails und deren Attachments.
	Heuristische Prüfung	Aktiviert den heuristischen Suchmodus. Mittels Heuristik können bisher unbekannte Viren auf Grundlage bestimmter Aktionsmuster und Verhaltensweisen, entdeckt werden. Dabei kann es auch zu Fehlalarmen kommen. Sollte eine verdächtige Datei auf Ihrem System gefunden werden, empfehlen wir, die Datei zur Überprüfung an das BitDefender-Virus-Labor zu schicken.
	Unvollständige Virenkörper	Spürt unvollständige Virenkörper auf.

- Legt das Ziel für einen Spyware-Prüfvorgang fest (laufende Prozesse, Cookies und/oder Arbeitsspeicher). Weitere Optionen können über die Kategorie **Spyware Prüfoptionen** angegeben werden.

Option	Beschreibung
Systemregistrierung prüfen	Prüft Einträge in der Systemregistrierung.

Option	Beschreibung
Cookies prüfen	Prüft gespeicherte Cookies von Webseiten.

- Wählen Sie die Aktionen für infizierte und verdächtige Dateien aus. Öffnen Sie die **Aktionsoptionen**, um alle möglichen Aktionen für diese Dateien anzeigen zu lassen.

  Wählen Sie die Aktion, die durchzuführen ist, wenn eine infizierte oder verdächtige Datei gefunden wird. Sie können unterschiedliche Vorgehensweisen für infizierte und verdächtige Dateien festlegen. Sie können außerdem eine sekundäre Aktion festlegen, wenn die Primäre fehlschlägt.

Aktion	Beschreibung
Objekte protokollieren	Es wird keine Aktion für infizierte Dateien ausgeführt. Diese Dateien finden Sie Berichtsdatei.
Benutzer abfragen	Bei einer entdeckten Infektion muss der Benutzer die weiteren Aktionen bestätigen. Folgende Optionen stehen zur Verfügung: Desinfizieren, in der Quarantäne Isolieren oder Löschen.
Dateien reparieren	Um die infizierte Datei zu desinfizieren.
Dateien löschen	Die infizierte Datei wird ohne Warnung sofort gelöscht.
In die Quarantäne verschieben	Verschiebt die infizierte Datei in die Quarantäne.
Dateien umbenennen	Die infizierte Datei wird umbenannt. Die neue Erweiterung der infizierten Dateien wird `.vir` sein. Durch die Umbenennung von infizierten Dateien ist es nicht länger möglich, diese Dateien auszuführen, um somit eine weitere Verbreitung zu verhindern. Außerdem kann die Datei für weitere Analysezwecke gespeichert werden.



Wichtig

Umbenennen hat denselben Effekt auf versteckte Objekte (Rootkits). Die neue Erweiterung der Datei lautetnach diesem Vorgang `.bd.ren`. Durch die Umbenennung erkannter Dateien wird die Möglichkeit einer Ausführung reduziert und die Verbreitung im Betriebssystem reduziert. Des weiteren kann die Datei für weitere Analysen abgespeichert werden.

- Optionen für Berichtsdateien angeben. Öffnen Sie die **Berichtsoptionen** um alle möglichen Optionen anzeigen zu lassen.

Option	Beschreibung
Alle geprüften Objekte anzeigen	Zeigt in einer Berichtdatei den Status und mögliche Infektionen aller geprüften Dateien an. Ist diese Option aktiviert, so kann es zur Verlangsamung des Computers führen.
Berichte älter als (x) Tage löschen	In diesem Feld können Sie festlegen (wo möglich) wie lange ein Bericht gespeichert (erinnert, abgelegt, hinterlegt) werden soll Scan Logs section. Wählen Sie diese Option und geben Sie ein neues Zeitintervall ein. Die Standardeinstellung ist 180 Tage.



Anmerkung

Die Berichtsdatei kann im Abschnitt Berichte im Menüpunkt **Eigenschaften** eingesehen werden.



- Festlegen weiterer Optionen. Öffnen Sie den Abschnitt **Erweitert**, um folgende Optionen auszuwählen:

Option	Beschreibung
Versenden verdächtiger Dateien an das BitDefender Labor	Sie haben die Möglichkeit, verdächtige Dateien zur Prüfung an das BitDefender Labor zu schicken.

Mit dem Klick auf **Standard** laden Sie die Grundeinstellungen.

Klicken Sie auf **OK**, um die Änderungen zu speichern.

Andere Optionen

Eine Reihe von allgemeinen Optionen für den Prüfvorgang stehen ebenfalls zur Verfügung:

Option	Beschreibung
Aufgaben mit niedriger Priorität ausführen	Herabstufung der Priorität des Prüfvorgangs. Andere Programme werden somit schneller ausgeführt. Der gesamte Prüfvorgang dauert damit aber entsprechend länger.
Herunterfahren des Computers nach erfolgtem Prüfvorgang	Der Rechner wird nach erfolgtem Prüfvorgang ausgeschaltet.
Versenden verdächtiger Dateien an das BitDefender Labor	Sie haben die Möglichkeit, verdächtige Dateien zur Prüfung an das BitDefender Labor zu schicken.
Minimieren des Prüffensters beim Scan-Start	Es verkleinert das Prüffenster beim Prüfvorgang in die untere Symbolleiste. Es kann durch einen Doppelklick auf das BitDefender – Logo in der Symbolleiste wieder geöffnet werden.

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Prüfen** klicken wird die Prüfung ausgeführt.

Prüfen der Zielobjekte

Klicken Sie auf die ausgewählte Aufgabe und dann auf den Reiter **Prüfpfad** um in diesen Abschnitt zu kommen.



Prüfen der Zielobjekte

Hier können Sie den Prüfpfad festlegen.

Dieser Bereich enthält folgende Schaltflächen:

- **Datei hinzufügen** - diese Schaltfläche ermöglicht das Hinzufügen bestimmter, zu prüfender Dateien. Wenn Sie hierauf klicken, können Sie die Dateien im nächsten sich öffnenden Fenster auswählen.
- **Ordner hinzufügen** - diese Schaltfläche ermöglicht das Hinzufügen eines neuen, zu prüfenden Ordners. Wenn Sie hierauf klicken, können Sie den Ordner im nächsten, sich öffnenden Fenster auswählen.



Anmerkung

Ziehen Sie per Drag & Drop Dateien und Ordner auf die Prüfen-Sektion, um diese der Liste der zu prüfenden Objekte zuzufügen.

- **Eintrag löschen** - löscht die Datei/denOrdner, die/der vorher ausgewählt wurde.



Anmerkung

Nur die Dateien/Ordner, die nachträglich hinzugefügt wurden, können gelöscht werden. Dateien/Ordner, die von BitDefender vorgegeben wurden, können nicht gelöscht werden.

Optionen, die das schnelle Auswählen der Scan-Ziele erlauben.

- **Lokale Laufwerke** - prüft die lokalen Laufwerke.
- **Netzlaufwerke** - prüft die verfügbaren Netzwerklaufwerke.
- **Wechseldatenträger** - prüft alle entfernbaren Laufwerke (CD-ROM-Laufwerke, Diskettenlaufwerke, USB-Sticks).
- **Alle Laufwerke** - prüft alle Laufwerke: lokale, entfernbare oder verfügbare Netzwerklaufwerke.



Anmerkung

Zur schnellen Auswahl aller Laufwerke klicken Sie auf **Alle Laufwerke** auswählen.

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Prüfen** klicken wird die Prüfung ausgeführt.

Zeitgesteuertes Starten von Prüfvorgängen

Über den Abschnitt **Zeitgesteuerte Aufgaben** können Sie beliebige Zeiten für den Scanvorgang festlegen.



Zeitgesteuertes Starten von Prüfvorgängen

Hier können Sie nachsehen, ob eine Aufgabe geplant ist oder nicht und Sie können die Eigenschaften ändern.



Wichtig

Während umfassender Prüfungen kann der Prüfprozess eingige Zeit in Anspruch nehmen und läuft reibungslos, wenn Sei währenddessen alle anderen Programme schließen. Aus diesem Grunde ist es ratsam die Prüfvorgänge zu planen, wenn Sie Ihren Computer nicht nutzen oder er im Standby Modus ist.

Wenn Sie Prüfvorgänge planen müssen Sie eine der folgenden Optionen auswählen:

- **nicht geplant** - führt den Scan nur auf Anfrage des Nutzers hin durch.
- **Einmal** - führt den Scan nur einmal, zu einem bestimmten Zeitpunkt aus. Definieren Sie den Startzeitpunkt im Feld **Start Datum/Zeit**.
- **Periodisch** - startet den Prüfvorgang in festgelegten Zeitabständen (Stunden, Tage, Wochen, Monate, Jahre) beginnend mit einem fest definierten Zeitpunkt (Datum und Uhrzeit).

  Wenn der Scanvorgang nach einem bestimmten Zeitraum wiederholt werden soll, aktivieren Sie das Kontrollkästchen **Regelmäßig**, und geben Sie in das Textfeld **Alle** die entsprechende Anzahl von Minuten/Stunden/Tage/Wochen/Monate/Jahre ein, nach der die Wiederholung erfolgen soll. Definieren Sie den Startzeitpunkt im Feld **Start Datum/Zeit**.

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Prüfen** klicken wird die Prüfung ausgeführt.

Prüfberichte

Klicken Sie auf due ausgewählte Aufgabe und wählen Sie **Berichtsdateien** um in diesen Abschnitt zu gelangen.



Prüfberichte

Hier können Sie nach jeder durchgeführten Prüfung die Berichtsdateien einsehen. Jede Datei beinhaltet Informationen über den Status (sauber/infiziert), das Datum und die Zeit wann die Prüfung durchgeführt wurde und eine Zusammenfassung (Prüfung beendet).

Zwei Schaltflächen sind verfügbar:

- **Anzeigen** - öffnet die ausgewählte Berichtsdatei;
- **Löschen** - löscht die ausgewählte Berichtsdatei;

Sie könne auch um eine Datei anzusehen oder zu löschen einfach mit einem rechten Mausklick die entsprechende Option aus dem Shortcut Menu auswählen.

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Prüfen** klicken wird die Prüfung ausgeführt.

7.2.3. Shortcut Menü

Für jede Aufgabe steht ein Shortcut Menü zur Verfügung. Mit einem rechten MAusklick könne Sie die ausgewählte Aufgabe öffnen:



Shortcut Menü



Folgende Aktionen stehen zur Verfügung:

- **Eigenschaften** - öffnet das Fenster **Eigenschaften**, **Übersicht** tab, wo Sie die Einstellungen für die ausgewählte Aufgabe ändern können;
- **Zielprüfung ändern** - öffnet **Eigenschaften** Fenster, **Prüfpfad** tab, wo Sie das Prüfziel für die ausgewählte Aufgabe ändern können.
- **Planen** - öffnet das Fenster **Eigenschaften** , **Planer**, wo Sie die ausgewählten Aufgaben planen können;
- **Prüfberichte anzeigen** - öffnet das Fenster **Eigenschaften** , **Prüfberichte**, wo Sie die Berichte sehen, die nach der Prüfung erstellt wurden.
- **Wiederholen** - wiederholt die ausgewählte Aufgabe.



Anmerkung

Dies ist sinnvoll, wenn neue Aufgaben erstellt werden, weil die Einstellungen für die wiederholte Aufgabe geändert werden können.

- **Shortcut auf den Desktop** - Erstellt einen Shortcut zum Desktop über die ausgewählte Aufgabe.
- **Löschen** - löscht die ausgewählte Aufgabe.

Anmerkung

Für Systemaufgaben nicht verfügbar. Sie können Systemaufgaben nicht löschen.

- **jetzt prüfen** - führt die ausgewählte Aufgabe aus und startet eine sofortige Prüfung.



Wichtig

Aufgrund ihrer speziellen Beschaffenheit können nur die Optionen **Eigenschaften** und **Berichtsdateien ansehen** unter dem Punkt **Verschiedene Aufgaben** ausgewählt werden.

7.2.4. On-Demand-Scanner.

BitDefender bietet drei verschiedene On-Demand-Scan-Typen:

- Sofortiges prüfen - folgen Sie den unten angegebenen Schritten, um Ihren Computer auf Viren zu prüfen;
- Kontextbezogenes Prüfen - Rechtsklick auf eine Datei oder einen Ordner und wählen Sie im Kontextmenü BitDefender AntiVirus v10 aus;
- Prüfen per Drag& Drop - verschieben Sie mittels Drag & Drop eine Datei oder einen Ordner auf die Aktivitäts-Anzeige;

Sofortiges Scannen

Um Ihren Computer oder Teile Ihres Computers zu prüfen können Sie die Standardeinstellungen nutzen oder Ihre eigenen Aufgaben einrichten. Es gibt zwei Möglichkeiten Aufgaben einzurichten:

- Wiederholen einer existierenden Regel, neu benennen und machen Sie die nötigen Änderungen im Fenster Eigenschaften;
- Klicken Sie unter **Neue Aufgaben** auf Konfigurieren,.

Damit Sie einen vollständigen Suchlauf mit BitDefender durchführen können, ist es wichtig, alle Programme zu beenden. Besonders wichtig ist, dass Sie Ihr E-Mail Programm schließen (z. B. Outlook, Outlook Express oder Eudora).

Da es täglich neue Bedrohungen durch Viren und Würmer gibt, sollten Sie, bevor Sie den Suchlauf starten, BitDefender mit Hilfe des Update Moduls aktualisieren.

Um die Prüfung zu starten wählen Sie die gewünschten Prüfaufgaben aus der Liste aus und klicken Sie **Jetzt prüfen** auf dem rechten Button. Sie könne auch auf den Button **Aufgabe ausführen** klicken. Das Prüffenster wird dann geöffnet:



Prüffenster

Es wird ein Symbol in der Symbolleiste angezeigt, wenn ein Prüfvorgang aktiv ist.

Während des Prüfvorgangs wird BitDefender den Fortschritt anzeigen und Sie benachrichtigen, wenn Bedrohungen gefunden wurden. Auf der rechten Seite können Sie die Statistiken des Prüfvorgangs sehen. Abhängig von der ausgewählten Prüf-Option (Spyware oder Viren) sind Informationen verfügbar. Wenn beide Optionen verfügbar sind wählen Sie die dementsprechenden Informationen aus um mehr über den Prüfvorgang nach Spyware oder Viren zu erfahren.

Wählen Sie die Checkbox **Zuletzt geprüfte Dateien anzeigen** und Sie sehen nur Informationen über die zuletzt geprüften Dateien.



Anmerkung

Der Prüfvorgang kann, abhängig von der Größe Ihrer Festplatte, einen Moment dauern.

Drei Schaltflächen sind verfügbar:

- **Stopp** - Ein neues Fenster öffnet sich und Sie werden gefragt, ob Sie die Systemprüfung stoppen möchten. Klicken Sie auf **Ja**&**Schließen**, um das Fenster und den Prüfvorgang zu schließen.
- **Pause** - Hält den Prüfvorgang für eine bestimmte Zeit an; klicken Sie auf **Fortsetzen**, um ihn wieder zu starten.
- **Bericht anzeigen** - Der Prüfbericht wird geöffnet und die zurzeit überprüften Dateien werden laufend angezeigt.

Anmerkung

Mit einem rechten Mausklick auf eine laufende Aufgabe, einen Shortcut (kontext) Menü erscheint das Prüffenster. Die Optionen (**Pause / Fortsetzen**, **Stop** und **Stoppen und schließen**)sind den Buttons des Prüffensters ähnlich.



Wenn die Einstellung **Eingabeaufforderung** eingestellt ist im Fenster Properties , wird ein Fenster geöffnet, in dem Sie aufgefordert werden die Aktion auszuwählen, die im Falle einer infizierten Datei ausgeführt werden soll.



Auswahl für Aktionen

Sie sehen den Namen der Datei und den Namen des Virus.

Nun können Sie eine der folgenden Möglichkeiten auswählen:

- **Desinfizieren** - reinigt die infizierten Dateien;
- **Löschen** - löscht automatisch alle infizierten Dateien, ohne eine Warnmeldung auszugeben;
- **In Quarantäne verschieben** - verschiebt die infizierten Dateien in die Quarantäne;
- **Ignorieren** - In diesem Fall wird die Infizierung ignoriert und keine Aktion ausgeführt.

Wenn Sie einen gesamten Ordner überprüfen und die ausgewählte Aktion auf alle gefundenen Schädlinge übertragen möchten, so wählen Sie bitte die Option **Für alle anwenden**.



Anmerkung

Ist die Option **Desinfizieren** nicht verfügbar, so bedeutet dies, das die Datei nicht desinfiziert werden kann. Die beste Alternative ist, die Datei in der Quarantäne zu isolieren und diese später zwecks Analyse an das Virenlabor zu senden.

Klicken Sie auf **OK**.



Anmerkung

Die Berichtsdatei wird automatisch im Abschnitt Berichte im Menüpunkt **AntiVirus** gesichert.

Scannen mit dem Kontextmenü

Klicken Sie mit der rechten Maustaste auf die zu prüfende Datei. Wählen Sie **BitDefender Antivirus v10** aus.



Kontextmenü

Sie können die Prüfoptionen ändern und die Berichtsdatei einsehen, wenn Sie im Fenster Eigenschaften auf **Prüfen Kontext Menü** klicken.

Prüfen per Drag & Drop

Ziehen Sie die gewünschte Datei auf den **Datei-/Netzprüfmonitor**, wie auf den folgenden Bildern dargestellt.



Herüberziehen der Datei



Ablegen der Datei

Wenn eine infizierte Datei entdeckkt wurde erscheint ein Alarm Fenster und fragt welche Aktion durchgeführt werden soll.

In beiden möglichen Prüfalternativen (Kontext Menü und drag&drop) erscheint Prüffenster .

7.2.5. Prüfen auf Rootkits

Mit der neu eingeführten Antirootkit-Technologie wird die Effizienz von BitDefender noch einmal gesteigert. Dadurch ist BitDefender nun in der Lage Rootkits aufzuspüren und unschädlich zu machen.

Um Ihren Computer auf Rootkits zu prüfen starten Sie bitte den Task **Auf Rootkits prüfen**. Anschließend erscheint das Prüffenster.





Wichtig

Es wird empfohlen keine Aktion auf versteckte Objekte anzuwenden wenn BitDefender den Computer auf Rootkits überprüft.

Am Ende eines jeden Prüfvorgangs bekommen Sie den Prüfbericht angezeigt. Überprüfen Sie gefundene, versteckte Objekte sorgfältig: Das Vorhandensein von solchen ist eventuell ein Indikator für ein kompromitiertes System.

Wenn Sie sicher sind das es sich bei einer erkannten Datei um Malware handelt, empfehlen wir Ihnen die Aktion auf **Umbenennen** zu stellen und erneut die Aufgabe **Auf Rootkits prüfen** durchzuführen. So stellen Sie sicher, dass die versteckten Dateien unbrauchbar gemacht werden.



Warnung

WARNUNG: NICHT ALLE VERSTECKTEN OBJEKTE SIND MALWARE! Stellen Sie vor dem Umbenennen-Vorgang sicher, dass die jeweiligen Objekte nicht zu einer auf dem Computer installierten, legitimen Anwendung gehören. Ein Umbenennen solch einer Datei kann Ihr System unbrauchbar machen.



Wichtig

Ist ein Computer erst einmal durch ein Rootkit kompromitiert worden, gibt es lediglich eine Lösung um diesen vollständig zu säubern: Eine Neuinstallation des Betriebssystems.

7.3. Quarantäne

Um diese Sektion zu öffnen klicken Sie bitte auf **Quarantäne** im Modul **Antivirus**.



Quarantäne

Mit BitDefender können Sie infizierte oder "verdächtige" Dateien in einem sicheren Bereich, der als Quarantäne bezeichnet wird, isolieren. Durch das Isolieren dieser Dateien in einem Quarantänebereich wird das Infektionsrisiko eliminiert und gleichzeitig können diese Dateien zu weiteren Analysezwecken an das BitDefender Lab gesendet werden.

Der Bestandteil, der die Verwaltung der isolierten Dateien sicherstellt, ist die **Quarantäne**. Dieses Modul enthält eine Funktion, die die infizierten Dateien auf Wunsch automatisch zum BitDefender-Labor sendet.

Wie Sie sicherlich bereits festgestellt haben, enthält der Abschnitt **Quarantäne** eine Liste aller Dateien, die isoliert wurden. Zu jeder Datei sind die folgenden Informationen verfügbar: Name, Dateigröße, Isolationsdatum und Übertragungsdatum. Um weitere Informationen anzuzeigen, klicken Sie bitte auf **Mehr Infos**.



Anmerkung

Die in der Quarantäne enthaltenen Dateien können weder ausgeführt noch geöffnet werden.

Klicken Sie **Hinzufügen** um eine verdächtige Datei zur Quarantäne hinzuzufügen. Es öffnet sich dann ein Fenster und Sie können die Datei auf dem Laufwerk auswählen. Dann wird die Datei in Quarantäne kopiert. Wenn die Datei in Quarantäne geschoben werden soll wählen Sie **löschen in ursprünglicher Speicherstelle** . Ein schnellerer Weg eine verdächtige Datei zur Quarantäne hinzuzufügen ist drag&drop sie in die Quarantäne.

Um eine ausgewählte Datei aus der Quarantäne zu löschen klicken Sie the **entfernen**. Wenn Sie eine infizierte Datei wiederherstellen wollen in ihrem original Speicherort klicken Sie **Wiederherstellen**.

Sie können jede ausgewählte Datei aus der Quarantäne in das BitDefender labor senden in dem Sie **Senden** klicken.



Wichtig

Sie müssen zunächst weitere Informationen angeben, bevor Sie Dateien übertragen. Klicken Sie zunächst auf **Einstellungen** und füllen Sie dort das Feld **E-Mail-Adresse** aus.

Click **Einstellungen** um die erweiterten Optionen für die Quarantäne zu öffnen. Das folgender Fenster erscheint:



Quarantäne-Einstellungen

Die Quarantäne-Einstellungen sind in zwei Kategorien unterteilt:

- **Allgemein**
- **Übertragungs-Einstellungen**

Anmerkung

Klicken Sie auf "+", um eine Option zu öffnen, und auf "-", um diese zu schließen.



Allgemein

- **Größe der Quarantäne begrenzen** - Hält die Größe der Quarantäne unter Kontrolle. Diese Option ist in der Voreinstellung aktiviert und liegt bei 12.000 KB. Wenn Sie diesen Wert ändern möchten, klicken Sie bitte in das Eingabefeld und tragen Sie einen neuen Wert ein. Wenn Sie das Ankreuzfeld **Alte Dateien automatisch löschen** auswählen und das Quarantäne-Verzeichnis die maximale Größe erreicht hat, werden automatisch die ältesten Dateien gelöscht, um den verwendeten Speicherplatz für neuere Dateien freizugeben.
- **Automatisches Versenden der Quarantäne** - sendet automatisch alle Dateien aus dem Quarantäne-Ordner zur Überprüfung an das BitDefender-Virenlabor. Sie können das Intervall bestimmen, in dem der **Inhalt der Quarantäne automatisch versendet wird**.
- **Gesendete Dateien automatisch löschen** - löscht automatisch die aus der Quarantäne gesendeten Dateien.
- **Drag & Drop settings** - für die Drag & Drop-Funktion des Quarantäne-Ordners können Sie hier die Art des Drag & Drop einstellen: Kopieren der Dateien, Verschieben der Dateien, Benutzer abfragen.

Übertragungs-Einstellungen

- **Ihre E-Mail-Adresse** - geben Sie hier Ihre E-Mail-Adresse an, wenn Sie eine Antwort bezüglich der eingesendeten Dateien aus dem Virenlabor haben möchten.

Klicken Sie auf **OK** um die Einstellungen zu speichern. Wenn Sie auf **Standard** klicken werden die Werkseinstellungen geladen.



8. Das Modul Antispyware

Der Abschnitt **AntiSpyware** behandelt und erklärt folgende Themen:

- Status der AntiSpyware
- Privacy Kontrolle
- Registrierung prüfen
- Anwahl-Kontrolle
- Cookie-Kontrolle
- Skript-Kontrolle
- System-Informationen

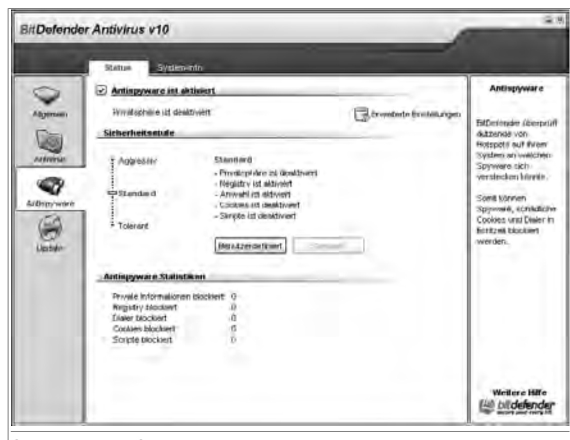


Anmerkung

Weitere Inhalte und Einzelheiten zum Modul **AntiSpyware** finden Sie in der Produktbeschreibung auf Seite „*Das Modul Antispyware*“ (S. 15).

8.1. Status der AntiSpyware

Um diese Sektion zu öffnen klicken Sie bitte auf **Status** im Modul **Antispyware**.



Status der AntiSpyware

In dieser Sektion können Sie das **AntiSpyware**-Modul konfigurieren und Informationen über seine Einstellungen erhalten.



Wichtig

Um sicherzustellen, dass keine Spyware Ihren Computer infiziert, halten Sie das **Schutzschild** bitte immer aktiviert.

Am Schluss dieser Sektion können Sie die Statistiken einsehen.

Das **Spyware Schutzschild** schützt Ihren Computer vor Spyware durch 5 wichtige Kontrollmechanismen.

- Privacy Control - schützt Ihre vertraulichen Daten indem aller ausgehender HTTP und SMTP Datenverkehr aufgrund der erstellten Regeln Privacy geprüft wird.
- Registry Control - fragt um Erlaubnis immer wenn ein Programm versucht die Registry zu ändern um beim Windows Neustart ausgeführt zu werden.
- Dial Control - Fragt um Erlaubnis immer wenn ein Dialer versucht sich in den Computer einzuwählen.
- Hier hilft Ihnen die **Cookie-Kontrolle**. Wenn Sie aktiviert ist, wird die **Cookie-Kontrolle** bei jedem Versuch einer Webseite, einen Cookie anzubringen, Ihr diesbezügliches Einverständnis abfragen:
- Mit der **Skript Kontrolle** entscheiden Sie, welche Webseiten Sie als zuverlässig erachten und welche nicht. BitDefender wird immer Ihr Einverständnis abfragen, wenn eine Webseite ein Skript oder einen anderen aktiven Inhalt aktivieren will:

Um diese Einstellungen zu konfigurieren klicken Sie Erweiterte Einstellungen.

8.1.1. Sicherheitseinstellung

Sie können die Sicherheitseinstellung an Ihre Anforderungen anpassen. Ziehen Sie die Anzeige auf der Scala auf die richtige Einstellung.

Es gibt 3 mögliche Einstellungen:

Sicherheitseinstellung	Beschreibung
Zulassen	**Registrierung** aktiviert.
Standardeinstellung	**Registry Kontrolle** und **Dialer Kontrolle** sind aktiviert.
Aggressiv	**Registry Kontrolle**, **Dialer Kontrolle** und **Privacy Control** sind aktiviert.

Das Sicherheitslevel kann mit einem Klick auf **Benutzerdefiniert** angepasst werden. In einem neuen Fenster können Sie nun die Einstellungen anpassen und anschließend mit **OK** bestätigen.

Mit dem Klick auf **Standard** laden Sie die Grundeinstellungen.



8.2. Erweiterte Einstellungen - Privacy Kontrolle

Um auf diesen Bereich zuzugreifen klicken Sie **Erweiterte Einstellungen** im Feld **Antispyware Modul**, Status.



Privacy-Kontrolle

Vertrauliche Daten zu sichern ist für alle Anwender äußerst wichtig. Datenklau hat mit der Entwicklung der Internet Kommunikation standgehalten und wendet immer wieder neue Methoden an um Anwender zu täuschen und private Informationen zu erhalten.

Ob es sich um Ihre E-Mail Adresse handelt oder um Ihre Kreditkartennummer, wenn sie in die falschen Hände geraten können diese Informationen großen Schaden anrichten: Sie werden möglicherweise in Spam Mails ertrinken oder sich über ein geleertes Konto wundern.

Privacy Kontrolle hilft Ihre privaten Daten zu sichern. Sie prüft den HTTP oder SMTP Datenverkehr, oder beides, für spezielle Strings, die Sie definieren. Wenn eine Übereinstimmung gefunden wird, mit einer Internet Seite oder einer E-Mail Adresse, werden diese sofort geblockt.

Die Regeln können automatisch (durch das Fenster „Alarm“) oder manuell (bitte klicken Sie dazu **Hinzufügen**) erstellt werden und wählen Sie dann die entsprechenden Parameter aus.

8.2.1. Konfigurations-Assistent

Der Konfigurationsassistent wird in 3 Schritten eingestellt.

Schritt 1/3 - Typ und Richtung auswählen



Typ und Richtung auswählen

Geben Sie den Namen der Regel im Bearbeitungsfeld ein.

Hier können Sie die Parameter auswählen:

- **Regeltyp** - wählen Sie die Regel aus (Adresse, Name, Kreditkartennummer, PIN, TAN etc).
- **Regel für Daten** - Geben Sie die Regel für Daten ein.

Alle Daten, die Sie eingeben sind verschlüsselt. Um wirklich sicher zu gehen, geben Sie nicht alle Daten ein, die Sie schützen möchten.

Klicken Sie auf **Weiter**.

Schritt 2/3 - Datenverkehr auswählen



Datenverkehr auswählen

Bitte wählen Sie den verwendeten Netzwerktypen bzw. die Internetverbindung. Die folgenden Optionen stehen Ihnen zur Verfügung:

- **HTTP prüfen** - prüft den HTTP (web) Datenverkehr und blockiert ausgehende Daten, die den Regeln entsprechen.
- **Ausgehende E-Mails prüfen** - prüft alle ausgehenden E-Mail-Nachrichten.



Klicken Sie auf **Weiter**.

Schritt 3/3 – Beschreibung der Regel



Beschreibung der Regel

Geben Sie eine kurze Beschreibung der Regel im Eingabefeld ein.

Klicken Sie auf **Fertigstellen**.

Sie können eine Liste der Regeln in der Aufstellung ansehen.

Um eine Regel zu löschen, wählen Sie sie einfach aus und klicken **Löschen**. Um eine Regel zu deaktivieren ohen sie zu löschen, entfernen Sie den Haken in der entsprechenden Checkbox.

Um eine Regel zu bearbeiten wählen Sie die Regel aus und klicken **Bearbeiten** oder machen Sie einen Doppelklick. Das folgende Fenster erscheint:



Regel bearbeiten

Hier können Sie Namen, Beschreibungen und Parameter der Regel ändern. (Typ, Daten und Datenverkehr). Klicken Sie **OK** um die Änderungen zu speichern.

Klicken Sie auf **OK**, um die Änderungen zu speichern.

8.3. Registry Kontrolle

Für diesen Bereich klicken Sie auf das Fenster **Advanced Antispyware Einstellungen** (gehen Sie auf **Antispyware** module, Status und klicken Sie **Erweiterte Einstellungen**) und klicken den Reiter **Registry**.



Registry Kontrolle

Ein sehr wichtiger Teil von Windows ist die **Registry**. Dort werden von Windows alle Einstellungen, installierten Programme, Nutzerinformationen und so weiter verwaltet.

Die **Registry** bestimmt u. a., welche Programme automatisch beim Start von Windows geladen werden. Viren versuchen häufig hier anzusetzen, damit auch sie automatisch mit geladen werden, wenn der Nutzer seinen Computer startet.

Registry Kontrolle beobachtet die Windows-Registry – dies ist auch sehr hilfreich beim Aufspüren von Trojanern. Sie werden alarmiert, wann immer ein Programm versucht, einen Eintrag in die Registry zu unternehmen, um beim nächsten Windows-Start geladen zu werden.



Registry Alarm

Sie können die Änderung ablehnen, indem Sie auf **Nein** klicken, oder aber zulassen, indem Sie mit **Ja** bestätigen.

Wenn Sie möchten, dass BitDefender Ihre Antwort speichern soll, wählen Sie die Option: **Diese Antwort merken** aus.



Anmerkung

Wählen Sie Ja oder Nein auf der Grundlage Ihrer eigenen Sicherheitsrichtlinien.

Um einen Registry-Eintrag zu löschen, klicken Sie auf **Löschen**. Um zeitweise einen Registry Eintrag zu deaktivieren, ohne ihn zu löschen, entfernen Sie das Häkchen, indem Sie auf es klicken.



Anmerkung

BitDefender wird Sie bei der Installation neuer Programme informieren, wenn ein automatisches Starten nach der Windowsanmeldung erforderlich ist. In den meisten Fällen sind diese Programme legal und Sie können ihnen vertrauen.

Klicken Sie auf **OK**, um dieses Fenster zu schließen.

8.4. Erweiterte Einstellungen - Dialer Kontrolle

Für diesen Bereich klicken Sie auf das Fenster **Erweiterte Antispyware Einstellungen** (gehen Sie auf **Antispyware** module, Status und klicken Sie **Erweiterte Einstellungen**) und klicken den Reiter **Anwahl**.



Anwahl-Kontrolle

So genannte Dialer sind Anwendungen, die über Computer-Modems verschiedene Telefonnummern anwählen. Normalerweise werden Dialer genutzt, um unbemerkt kostenintensive Telefonnummern anzuwählen.

Mit der **Anwahl-Kontrolle** entscheiden Sie, welche Verbindung mit welcher Telefonnummer Sie zulassen oder unterbinden wollen. Die Anwahl-Kontrolle überwacht alle Dialer, die auf ein Computer-Modem zugreifen wollen, warnt den Benutzer unmittelbar und verlangt die Ablehnung oder Zustimmung zu solch einer Operation:



Anwahl-Alarme

Sie sehen den Namen der Anwendung und die vorgesehene Telefonnummer.

Wählen Sie **Diese Antwort merken** und klicken Sie auf **Ja** oder **Nein** und eine Regel wird erstellt, angewendet und in der Regelliste aufgenommen. Bei einer Wiederholung dieser Anwahl werden Sie nicht mehr informiert.

Jede erstellte Regel kann später über **Anwahl** aufgerufen und weiter bearbeitet werden.



Wichtig

Die Regeln sind nach Prioritäten gelistet. Dies bedeutet die erste Regel besitzt die höchste Priorität in der Liste. Per Drag & Drop können die einzelnen Regeln gemäß der gewünschten Priorität verschoben werden.

Um eine Regel zu löschen, wählen Sie diese aus und klicken Sie auf **Regel löschen**. Um eine Regel anzupassen doppelklicken Sie auf diese. Um eine Regel zeitweise zu deaktivieren ohne diese zu löschen, entfernen Sie die Markierung aus dem nebenstehende Kästchen durch anklicken.

Die Regeln können automatisch (durch das Fenster „Alarm“) oder manuell (bitte klicken Sie dazu **Hinzufügen**) erstellt werden und wählen Sie dann die entsprechenden Parameter aus.

8.4.1. Konfigurations-Assistent

Der Konfigurations-Assistent besteht aus zwei Schritten.

Schritt 1/2 - Anwendung und Aktion auswählen



Anwendung und Aktion auswählen

Hier können Sie die Parameter auswählen:

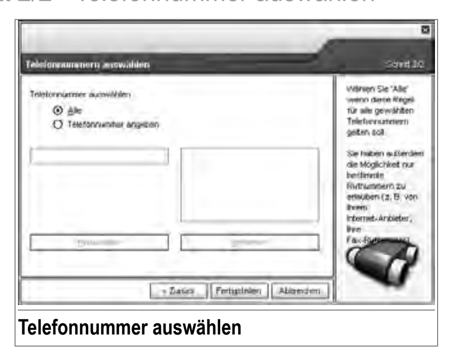


- **Anwendung** - wählen Sie die Anwendung für die Regel. Sie können eine bestimmte Anwendung wählen (klicken Sie **Anwendung auswählen**, **Durchsuchen** und wählen Sie eine bestimmte Anwendung) oder alle Anwendungen (markieren Sie **Alle**).
- **Aktion** - wählen Sie die Aktion der Regel.

Aktion	Beschreibung
Zulassen	Die Aktion wird erlaubt.
Verweigern	Die Aktion wird verweigert.

Klicken Sie auf **Weiter**.

Schritt 2/2 - Telefonnummer auswählen



Telefonnummer auswählen

Markieren Sie **Telefonnummer angeben**, geben Sie die Telefonnummer, für welche die Regel erstellt werden soll, in das darunter liegende Feld ein und klicken Sie auf **Hinzufügen**.



Anmerkung

Sie können Platzhalter in Ihrer Liste von nicht erlaubten Telefonnummern verwenden, z.B. : 1900* bedeutet, dass alle mit 1900 beginnenden Telefonnummern blockiert werden.

Markieren Sie **Alle**, falls diese Regel für alle Telefonnummern gelten soll. Falls Sie eine Nummer löschen möchten, wählen Sie diese aus und klicken Sie auf **Entfernen**.



Anmerkung

Sie können ebenfalls eine Regel definieren, die einem bestimmten Programm nur erlaubt, bestimmte Telefonnummern zur Anwahl zu verwenden (zum Beispiel die Ihres Internet-Providers oder Ihres Fax- oder News-Services).

Klicken Sie auf **Fertigstellen**.

Klicken Sie auf **OK**, um die Änderungen zu speichern.

8.5. Erweiterte Einstellungen

Um diesen Bereich zu bearbeiten klicken Sie **Erweiterte Antispyware Einstellungen**(gehen Sie auf **Antispyware** Modul, Status und klicken Sie **Erweiterte Einstellungen**) und klicken den Reiter **Cookie**.



Cookie-Kontrolle

Cookies werden von den meisten Webseiten im Internet verwendet. Es sind kleine Dateien, die auf Ihrem Computer gespeichert werden. Webseiten verschicken diese Cookies, um das Surfen zu beschleunigen, aber auch um Informationen über Sie zu erhalten.

Generell erleichtern Cookies das tägliche Internet-Leben. Zum Beispiel ermöglichen sie einer Webseite, Ihren Namen und sonstige Angaben zu speichern, so dass Sie diese nicht bei jedem Besuch eingeben müssen.

Cookies können jedoch auch missbräuchlich verwendet werden und Ihre Privatsphäre gefährden, indem Ihre Surfdaten an Dritte weitergegeben werden.

Hier hilft Ihnen die **Cookie-Kontrolle**. Wenn Sie aktiviert ist, wird die **Cookie-Kontrolle** bei jedem Versuch einer Webseite, einen Cookie anzubringen, Ihr diesbezügliches Einverständnis abfragen:



Cookie Alarm

Der Name des Programms, das versucht einen Cookie zu senden, wird Ihnen angezeigt.

Wählen Sie **Diese Antwort merken** und klicken Sie auf **Ja** oder **Nein** und eine Regel wird erstellt, angewendet und in der Regelliste aufgenommen. Sie werden dann nicht wieder informiert, wenn Sie das nächste Mal mit derselben Seite in Verbindung treten.

So werden Sie bei der Unterscheidung von zuverlässigen und unzuverlässigen Webseiten unterstützt.





Anmerkung

Aufgrund der großen Anzahl von Cookies, die heute im Internet verwendet werden, kann die **Cookie-Kontrolle** zu Beginn sehr oft nachfragen. Sobald Sie die von Ihnen regelmäßig besuchten Seiten in die Regelliste aufgenommen haben, wird Ihr Surfen im Internet aber wieder wie zuvor sein.

Jede erstellte Regel kann später über den Reiter **Cookies** aufgerufen und weiter bearbeitet werden.



Wichtig

Die Regeln sind nach Prioritäten gelistet. Dies bedeutet die erste Regel besitzt die höchste Priorität in der Liste. Per Drag & Drop können die einzelnen Regeln gemäß der gewünschten Priorität verschoben werden.

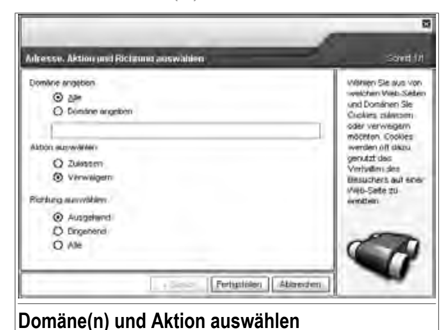
Um eine Regel zu löschen, wählen Sie diese aus und klicken Sie auf **Regel löschen**. Um eine Regel anzupassen doppelklicken Sie auf diese. Um eine Regel zeitweise zu deaktivieren ohne diese zu löschen, entfernen Sie die Markierung aus dem nebenstehende Kästchen durch anklicken.

Die Regeln können automatisch (durch das Fenster „Alarm“) oder manuell (bitte klicken Sie dazu **Hinzufügen**) erstellt werden und wählen Sie dann die entsprechenden Parameter aus.

8.5.1. Konfigurations-Assistent

Der Konfigurations-Assistent besteht aus einem einzelnen Schritt.

Schritt 1/1 - Domäne(n) und Aktion auswählen



Domäne(n) und Aktion auswählen

Hier können Sie die Parameter auswählen:

- **Domäne angeben** - schreiben Sie die Domäne, auf welche die Regel angewendet werden soll, in das darunter stehende Feld.
- **Aktion** - wählen Sie die Aktion der Regel.

Aktion	Beschreibung
Zulassen	Das Cookie dieser Domäne wird ausgeführt.
Verweigern	Das Cookie dieser Domäne wird nicht ausgeführt.

- **Richtung** - Wählen Sie die Richtung des Datenverkehrs aus.

Typ	Beschreibung
Ausgehend	Die Regel bezieht sich nur auf Cookies, welche von der verbundenen Seite versendet werden.
Eingehend	Die Regel bezieht sich nur auf Cookies welche an die verbundene Seite versendet werden.
Beide	Die Regeln finden in beide Richtungen Anwendung.

Klicken Sie auf **Fertigstellen**.



Anmerkung

Sie können Cookies akzeptieren, diese aber nicht zurücknehmen, indem Sie die Aktion **Verweigern** und die Richtung **Ausgehend** angeben.

Klicken Sie auf **OK**, um die Änderungen zu speichern.

8.6. Erweiterte Einstellungen

Um diesen Bereich zu bearbeiten klicken Sie **Erweiterte AntiSpyware Einstellungen** (gehen Sie auf **Antispyware** module, Status und klicken **Erweiterte Einstellungen**) und klicken den Reiter **Script**.



Skript-Kontrolle

Skripte und andere Programmierungen, wie z. B. ActiveX und Java applets, die für interaktive Webseiten verwendet werden, können verheerende Schäden verursachen. ActiveX-Elemente können zum Beispiel Zugriff auf Ihre Daten erlangen und sie auslesen, Daten von Ihrem Computer löschen, Passwörter auslesen und Nachrichten versenden, wenn Sie online sind. Sie sollten daher solche aktiven Elemente nur von Ihnen bekannten und zuverlässigen Seiten akzeptieren.

BitDefender ermöglicht Ihnen die Auswahl solche Elemente zuzulassen oder deren Ausführung zu blockieren.

Mit der **Skript Kontrolle** entscheiden Sie, welche Webseiten Sie als zuverlässig erachten und welche nicht. BitDefender wird immer Ihr Einverständnis abfragen, wenn eine Webseite ein Skript oder einen anderen aktiven Inhalt aktivieren will:





Skript Alarm

Der Namen der Quelle wird Ihnen angezeigt.

Wählen Sie **Diese Antwort merken** und klicken Sie auf **Ja** oder **Nein** und eine Regel wird erstellt, angewendet und in der Regelliste aufgenommen. Falls die gleiche Seite erneut Ihren aktiven Inhalt versenden will, werden Sie nicht wieder informiert.

Jede erstellte Regel kann später über den Reiter **Skripte** aufgerufen und weiter bearbeitet werden.



Wichtig

Die Regeln sind nach Prioritäten gelistet. Dies bedeutet die erste Regel besitzt die höchste Priorität in der Liste. Per Drag & Drop können die einzelnen Regeln gemäß der gewünschten Priorität verschoben werden.

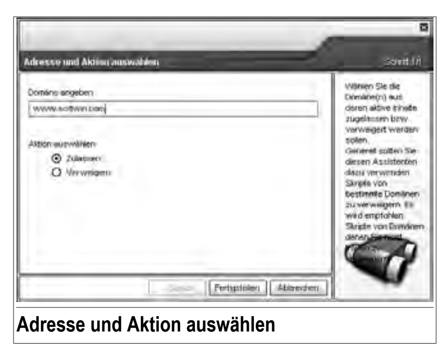
Um eine Regel zu löschen, wählen Sie diese aus und klicken Sie auf **Regel löschen**. Um eine Regel anzupassen doppelklicken Sie auf diese. Um eine Regel zeitweise zu deaktivieren ohne diese zu löschen, entfernen Sie die Markierung aus dem nebenstehende Kästchen durch anklicken.

Die Regeln können automatisch (durch das Fenster „Alarm“) oder manuell (bitte klicken Sie dazu **Hinzufügen**) erstellt werden und wählen Sie dann die entsprechenden Parameter aus.

8.6.1. Konfigurations-Assistent

Der Konfigurations-Assistent besteht aus einem einzelnen Schritt.

Schritt 1/1 - Adresse und Aktion auswählen



Adresse und Aktion auswählen

Hier können Sie die Parameter auswählen:

- **Domäne angeben** - schreiben Sie die Domäne, auf welche die Regel angewendet werden soll, in das darunter stehende Feld.
- **Aktion** - wählen Sie die Aktion der Regel.

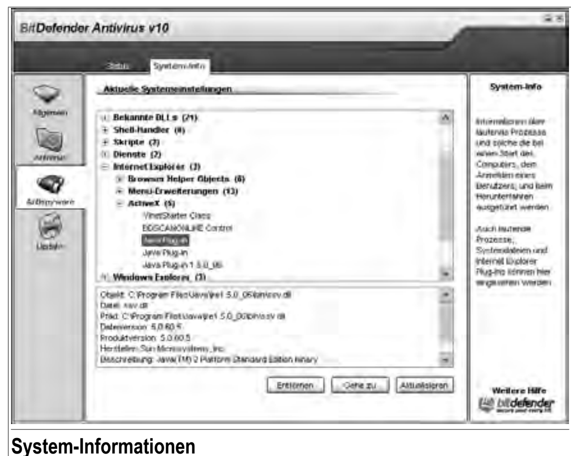
Aktion	Beschreibung
Zulassen	Die Scripts auf dieser Domäne werden ausgeführt.
Verweigern	Die Scripts auf dieser Domäne werden nicht ausgeführt.

Klicken Sie auf **Fertigstellen**.

Klicken Sie auf **OK**, um die Änderungen zu speichern.

8.7. System-Informationen

Um diese Sektion zu öffnen klicken Sie bitte auf **System-Info** im Modul **Antispyware**.



System-Informationen

In diesem Bereich können Sie Ihre Basiseinstellungen einsehen und verändern.

Die Auflistung enthält alle Einstellungen die angewendet werden, sowohl wenn der Computer gestartet wird als auch wenn spezielle Anwendungen aufgerufen werden und gesonderte Regeln besitzen.

Drei Schaltflächen sind verfügbar:

- **Löschen** - löscht das ausgewählte Objekt.
- **Gehe zu** - öffnet ein Fenster mit der Pfadangabe für das Objekt.
- **Aktualisieren** - öffnet erneut die das Menü **System-Info**.



9. Das Modul Update

Der Abschnitt **Update** behandelt und erklärt folgende Themen:

- Automatisches Update
- Manuelles Update
- Update-Einstellungen

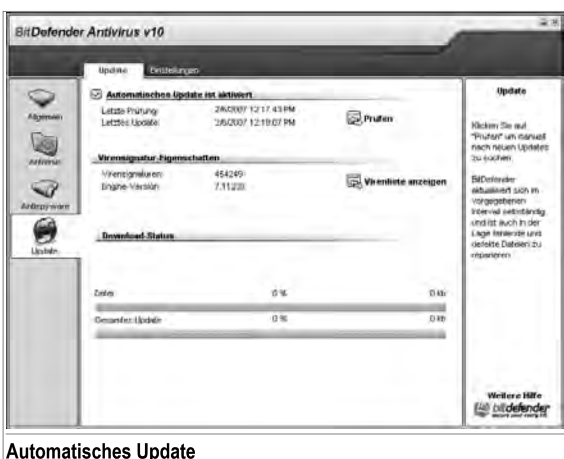


Anmerkung

Weitere Inhalte und Einzelheiten zum Modul **Update** finden Sie in der Produktbeschreibung auf Seite „*Das Modul Update*“ (S. 15).

9.1. Automatisches Update

Um diese Sektion zu öffnen klicken Sie bitte auf **Update** im Modul **Update**.



Automatisches Update

Hier finden Sie eine Übersicht über den Produkt-Status.



Wichtig

Um den Schutz vor Spyware aus dem Internet zu gewährleisten, halten Sie Ihre **Automatisches Update** Funktion jederzeit aktiviert.

Falls Sie über eine Breitbandverbindung oder eine DSL-Verbindung verfügen, arbeitet BitDefender eigenständig. Es prüft beim Start des Computers, ob neue Virensignaturen verfügbar sind und fährt nach Bedarf sogar **stündliche** Updates.

Wenn ein neues Update verfügbar ist, handelt BitDefender je nach vorgenommener Einstellung im Menü Einstellungen. Entweder werden Sie darum gebeten, den neu verfügbaren Download jetzt herunter zu laden oder das Update erfolgt automatisch.

Das automatische Update kann auch jederzeit über den Klick **Prüfen** erfolgen. Diese Funktion wird auch als **benutzergesteuertes Update** bezeichnet.

Das **Update** module Modul verbindet Ihren Computer mit dem BitDefender Update Server und benachrichtigt Sie bei einem neu verfügbaren Update. Wenn ein neues Update verfügbar ist, wird je nach vorgenommener Einstellung entweder darum gebeten, das Update Download jetzt herunter zu laden, oder das Update erfolgt automatisch.



Wichtig

Möglicherweise kann ein Neustart nach dem vollständig durchgeführten Update notwendig werden. Wir empfehlen Ihnen, den Neustart möglichst bald durchzuführen.



Anmerkung

Falls Sie über eine Internet by Call Verbindung verfügen, ist es sinnvoll, regelmäßig ein manuelles Update durchzuführen. Diese Vorgehensweise sollten Sie sich dann zu Eigen machen.

Sie können ein BitDefender Signaturen Update durchführen indem Sie klicken auf **Viren Liste**. Eine HTML Datei zeigt alle erstellten Signaturen. Klicken Sie noch mal **Viren Liste** um die Liste einzusehen. Sie können die Datenbank auf spezifische Signatur hin durchsuchen oder klicken Sie **BitDefender Virus Liste** um auf die online BitDefender Signaturen Datenbank zu gehen.

9.2. Manuelles Update

Diese Methode erlaubt Ihnen, durch die Installation der neusten Virensignaturen den bestmöglichen Virenschutz zu erhalten. Für die Installation des neusten Produktupdates wählen Sie bitte das automatische Update.



Wichtig

Nutzen Sie das manuelle Update, wenn das automatische Update nicht durchgeführt werden kann oder wenn der Computer nicht mit dem Internet verbunden ist.

Es gibt zwei mögliche Varianten, ein manuelles Update durchzuführen:

- Mit einer `weekly.exe` Datei;
- Mit einem `zip Archiv`.

9.2.1. Das manuelle Update mit der `weekly.exe` Datei

Das Update Paket `weekly.exe` wird jeden Freitag frei geschaltet und enthält alle neuen Virusdefinitionen und Prüfmechanismen bis zum Freigabedatum.

Um das BitDefender Update über die Datei `weekly.exe`, durchzuführen, folgen Sie den nächsten Schritten:

1. Herunterladen der weekly.exe und speichern dieser Datei lokal auf Ihrer Festplatte.
2. Rufen Sie die herunter geladene Datei auf und mit einem Doppelklick rufen Sie den Update Assistenten auf.
3. Klicken Sie auf **Weiter**.
4. Überprüfen Sie **Ich akzeptiere die Lizenzvereinbarungen** und klicken Sie auf **Weiter**.
5. Klicken Sie auf **Installieren**.
6. Klicken Sie auf **Fertigstellen**.



9.2.2. Das manuelle Update per `ZIP Archiv`

Auf dem Update-Server sind zwei Zip-Archive abgelegt, die die Updates für die Scan-Module bzw. für die Virensignaturen enthalten: `cumulative.zip` und `daily.zip`.

- Der `cumulative.zip` wird jede Woche montags veröffentlicht und beinhaltet alle neuen Virus Definitionen und Prüfmechanismen bis zum Datum der Veröffentlichung.
- Der `daily.zip` wird jeden Tag veröffentlicht und enthält alle neuen Virus Definitionen und Prüfmechanismen ausgehend von der letzten, erfolgten Zusammenstellung bis zum aktuellen Tag.

BitDefender verwendet eine servicebasierte Architektur. Aufgrund dieser Vorgehensweise ist die Erneuerung der Viren-Definitionen abhängig vom Betriebssystem:

- Windows 2000, Windows XP.
- Windows 98, Windows Millennium.

Windows 2000, Windows XP

Gehen Sie wie folgt vor:

1. **Herunterladen des richtigen Updates.** Laden Sie montags die Datei cumulative.zip herunter, und speichern Sie das Archiv auf der Festplatte. Laden Sie an anderen Tagen die Datei daily.zip herunter, und speichern Sie das Archiv auf der Festplatte. Wenn Sie zum ersten Mal ein manuelles Update durchführen, laden Sie beide Archive herunter.
2. **Beenden der BitDefender Virusschutzfunktion.**
   - **Verlassen Sie bitte die BitDefender Management Konsole.** Klicken Sie auf das BitDefender Symbol in der Systemleiste, und wählen Sie die Option **Beenden**.
   - **Öffnen der Dienste.** Klicken Sie auf **Starten**, dann auf **Systemsteuerung**, doppelklicken Sie auf **Verwaltung**, und klicken Sie auf **Dienste**.
   - **Stoppen des BitDefender Virus Schild.** Wählen Sie den Service **BitDefender Virus Schild** aus der angezeigten Liste und klicken sie auf **Stoppen**.
   - **Stoppen der BitDefender Scan Server.** Wählen Sie den Service **BitDefender Scan Server** aus der angezeigten Liste und klicken Sie auf **Stoppen**.
3. **Extrahieren der Archivinhalte.** Starten Sie bitte mit dem Archiv `cumulative.zip` sobald beide Archive verfügbar sind. Extrahieren Sie die Inhalte in das Verzeichnis `?:\Program Files\Common Files\Softwin\AV\Plugins` und bestätigen Sie das Überschreiben der bestehenden Dateien.
4. **Starten Sie den BitDefender Virenschutz wieder.**
   - **Starten des BitDefender Scan Server.** Wählen Sie **BitDefender Scan Server** in der angezeigten Liste und klicken Sie **Starten**.
   - **Starten des BitDefender Virus Schild.** Wählen Sie **BitDefender Virus Schild** von der angezeigten Liste und klicken Sie **Starten**.
   - **Öffnen Sie die BitDefender Management-Konsole.**

Windows 98, Windows Millennium

Gehen Sie wie folgt vor:

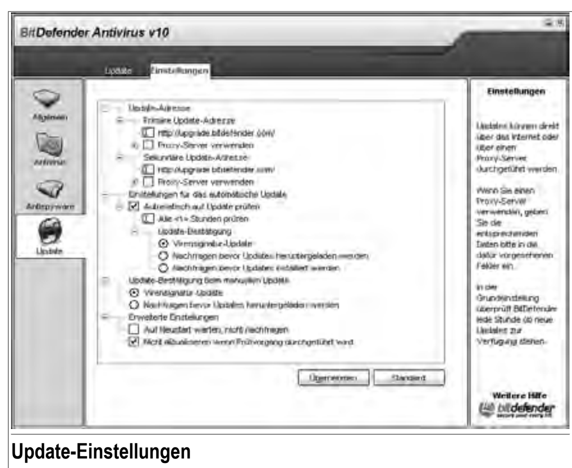
1. **Herunterladen des richtigen Updates.** Laden Sie montags die Datei cumulative.zip herunter, und speichern Sie das Archiv auf der Festplatte. Laden Sie an anderen Tagen die Datei daily.zip

herunter, und speichern Sie das Archiv auf der Festplatte. Wenn Sie zum ersten Mal ein manuelles Update durchführen, laden Sie beide Archive herunter.

2. **Extrahieren der Archivinhalte.** Starten Sie bitte mit dem Archiv `cumulative.zip` sobald beide Archive verfügbar sind. Extrahieren Sie die Inhalte in das Verzeichnis `?:\Program Files\Common Files\Softwin\AV\Plugins` und bestätigen Sie das Überschreiben der bestehenden Dateien.
3. **Bitte starten Sie Ihren Computer neu.**

9.3. Update-Einstellungen

Um diese Sektion zu öffnen klicken Sie bitte auf **Update** im Modul **Einstellungen**.



Update-Einstellungen

Die Updates können im lokalen Netzwerk, über das Internet, direkt oder über einen Proxy-Server durchgeführt werden.

Das Fenster mit den Update-Einstellungen enthält 4 aufklappbare Optionskategorien (**Update-Adresse**, **Automatisches Update**, **Update-Bestätigung beim manuellen Update** und **Erweiterte Einstellungen**), ähnlich wie in den Windowsmenüs.



Anmerkung

Klicken Sie auf eine Box mit einem "+", um ein Menü auszuklappen, und auf ein "-", um es zu schließen.

9.3.1. Update-Adresse

Für ein zuverlässigeres Update können zwei Update-Adressen angegeben werden. Ist die **primäre Adresse** nicht erreichbar, so wird auf der **sekundären Update-Adresse** nach verfügbaren Updates gesucht. Die folgenden Optionen sind verfügbar:

- **Ablagebereich für Updates** - bei einer Verbindung mit einem lokalen Netzwerk, in dem BitDefender Virendefinitionen lokal abgelegt werden, können Sie mit dieser Option den Pfad zum Ablageordner ändern. Standardmäßig lautet der Pfad: http://upgrade.bitdefender.com.



- **Proxy-Server verwenden** - Falls Sie einen Proxy-Server einsetzen, muss die entsprechende Markierung gesetzt werden. Nehmen Sie dann folgende Einstellungen vor:
  - **Adresse** - Geben Sie hier die IP-Adresse oder den Hostnamen des Proxy-Servers ein, den BitDefender verwendet.

    
    Wichtig
    Syntax: `name:port` oder `ip:port`.

  - **Benutzername** - Geben Sie den Benutzernamen ein, wenn der Proxy-Server eine Anmeldung erfordert.

    
    Wichtig
    Syntax: `domain\user`.

  - **Kennwort** - Geben Sie das Kennwort ein, wenn der Proxy-Server eine Anmeldung mit Kennwort erfordert.

9.3.2. Automatisches Update

- **Automatisch auf Update prüfen** - BitDefender verbindet sich automatisch mit dem BitDefender-Update-Server und prüft, ob neue Updates vorhanden sind.
- **Alle (1) Stunden prüfen** - Definiert, wie oft auf verfügbare Updates geprüft werden soll. Standard ist 1 Stunde.
- **Update im Hintergrund** - BitDefender führt Updates komplett selbständig durch.
- **Vor dem Herunterladen fragen** - BitDefender informiert den Benutzer vor dem Herunterladen der neuen Updates.
- **Vor der Installation fragen** - BitDefender informiert den Benutzer vor der Installation neuer Updates.

  
  Wichtig
  Wenn Sie die Optionen **Vor dem Herunterladen fragen** oder **Vor der Installation fragen** aktiviert haben und Sie die Management Konsole schließen und beenden, werden automatische Updates nicht durchgeführt.

9.3.3. Update-Bestätigung beim manuellen Update

- **Update im Hintergrund** - BitDefender führt Updates komplett selbständig durch.
- **Vor dem Herunterladen fragen** - BitDefender informiert den Benutzer vor dem Herunterladen der neuen Updates.


Wichtig
Wenn Sie die Optionen **Vor dem Herunterladen fragen** aktiviert haben und Sie die Management Konsole schließen und beenden, werden manuelle Updates nicht durchgeführt.

9.3.4. Erweiterte Einstellungen

- **Auf Neustart warten, nicht nachfragen** - Mit der Aktivierung dieser Einstellung wird der Benutzer nicht gefragt, ob ein Update durch Neustart durchgeführt werden soll. Somit wird der Benutzer während der Arbeit nicht durch BitDefender unterbrochen. Ohne Aktivierung teilt BitDefender mit, dass ein Update den Neustart des Computers benötigt und fragt den Benutzer ob der Neustart nun durchgeführt werden soll.
- **Nicht aktualisieren wenn Prüfvorgang durchgeführt wird** - BitDefender kann während des Prüfvorganges kein Update durchführen. Auf diese Weise kann der Update-Vorgang den Prüfvorgang nicht beeinflussen.



Anmerkung

Sollte BitDefender während eines Prüfvorganges aktualisiert werden, wird der Prüfvorgang abgebrochen.

Klicken Sie auf **Übernehmen** um die Einstellungen zu speichern. Wenn Sie auf **Standard** klicken werden die Werkseinstellungen geladen.



10. Empfohlene Vorgehensweisen

Der Abschnitt **Tipps und Tricks** behandelt und erklärt folgende Themen:

- Wie Sie Ihren Computer vor Malware Attacken schützen
- Konfigurieren der Prüfung

10.1. Wie Sie Ihren Computer vor Malware Attacken schützen

Folgen Sie diesen Schritten, um Ihren Computer gegen Viren, Spyware und andere Malware zu schützen.

1. **Beenden Sie den Installations-Assistenten.** Während der Installation erscheint der Installations-Assistent. Dieser wird Ihnenhelfen BitDefender zu registrieren und ein Benutzerkonto einzurichten, um vom Technischen Support zu profitieren. Er hilftaußerdem dabei zu prüfen, ob Ihr System sicher ist, indem ein Update und eine schnelle Systemprüfung gestartet wird. Es erlaubt ebenso eine tägliche komplette Systemprüfung.



Wichtig

Wenn Sie eine BitDefender Notfall CD haben, prüfen Sie Ihr System vor der BitDefender-Installation um sicher zu stellen, dass sich keine schädliche Software auf Ihrem Computer versteckt.

2. **Wie kann ich BitDefender aktualisieren?** Wenn Sie den Installations-Assistenten nicht beendet haben, starten Sie ein Update auf Anforderung (gehen Sie auf **Update** Modul, Update section, und klicken Sie **Jetzt Updaten**).
3. **Wie kann ich einen Prüfvorgang starten?** Gehen Sie in das Modul **Antivirus**, Shieldund klicken Sie **Jetzt prüfen**.

Anmerkung

Klicken Sie auf Prüfen um eine vollständige Systemprüfung zu starten und wählen Sie dort den Reiter **vollständige System Prüfung** und prüfen Sie **Aufgabe ausführen**.

4. **Infektion abwehren.** Halten Sie im Bereich **Virus Schild** die Option Echtzeit-Schutz aktiviert um in Echtzeit vor Schädlingen geschützt zu sein. Stellen Sie das Schutzlevel gemäß Ihren Bedürfnissen ein. Des weiteren können Sie auf Anpassen klicken um die Stufe selbst zu definieren.



Wichtig

Programmieren Sie den BitDefender Virenschutz so, dass Ihr System mindestens einmal pro Woche geprüft wird. Entsprechende Anleitungen finden Sie in diesem Handbuch unter „*Zeitgesteuertes Starten von Prüfvorgängen*“ (S. 43).

5. **Halten Sie Ihr BitDefender-Produkt auf dem neuesten Stand.** Im Modul **Update**, Update , aktiviern Sie bitte das **Automatische Update**ein, um optimal gegen die neuesten Bedrohungen geschützt zu sein.
6. **Eine komplette Systemprüfung planen.** Gehen Sie auf **Prüfen** und starten Sie BitDefender System Prüfung wenigstens einmal die Woche Planen the **Systemprüfung**

10.2. Konfiguration einer Prüfung

So richten Sie einen zeitgesteuerten Scanvorgang ein:

1. **Neue Aufgabe erstellen.** Im Abschnitt Prüfen und klicken Sie auf **Neue Aufgaben**. Das Fenster Einstellungen erscheint.

   Anmerkung

   Sie können auch neue Aufgaben erstellen mit Kopieren mit Hilfe einer bereits vorhandenen. Um das zu tun, gehen Sie mit dem rechten Mausklick auf Aufgabe und wählen Sie **Kopieren**im Shortcut menu. Doppelklick auf öffnen im Fenster **Eigenschaften**.

2. **Einstellen des Levels.** Gehen Sie in den Abschnitt **Übersicht** um den Level einzustellen. Wenn Sie möchten können Sie das Level anpassen unter Anpassen **Anpassen**.
3. **Weiterhin müssen Sie die Prüfart auswählen:** Gehen Sie im Abschnitt**Prüfpfad** auf auf wählen Sie die Objekte, die Sie prüfen wollen.
4. **Zeitgesteuerte Aufgaben.** Wenn die Aufgabe umfassend ist, sollten Sie die Prüfung auf später verschieben, wenn Ihr Computer im Stand-By Modus ist. Das gewährt eine korrekte Prüfung Ihres Systems durch BitDefender. Gehen Sie auf **Planen** zu Prüfung planen.



BitDefenderAntivirus v10 verfügt über eine bootfähige CD-ROM (BitDefender Notfall CD basierend auf LinuxDefender) die fähig ist, alle Festplatten zu prüfen und zu desinfizieren, bevor Ihr Betriebssystem startet.

Sie sollten die BitDefender Notfall CD immer dann verwenden, wenn Ihr System aufgrund von Virusinfektionen nicht mehr richtig funktioniert. Dies passiert für gewöhnlich, wenn Sie kein AntiVirus-Programm benutzen.

Das Update der Virensignaturen wird automatisch ohne Benutzereingriff jedes Mal vollzogen, wenn Sie die BitDefender Notfall CD starten.

LinuxDefender ist eine mit BitDefender erweiterte Knoppix-Distribution, welche die neueste Version von BitDefender für Linux in das GNU/Linux integriert. Es beinhaltet einen SMTP AntiVirus/AntiSpam-Schutz und einen On Demand Scanner, der in der Lage ist, Festplatten (inkl. Windows NTFS-Partition), Samba-Freigaben und NFS Mount Points zu überprüfen und zu desinfizieren. Eine web-basierte Konfigurationsschnittstelle zu den BitDefender-Lösungen ist ebenfalls enthalten.



11. Überblick

Aktuelle Bestandteile

- Direkte Überprüfung von E-Mails (AntiVirus & AntiSpam)
- AntiVirus-Lösungen für Ihre Festplatten
- NTFS Schreib-Unterstützung (über Captive-Projekt)
- Desinfektion infizierter Dateien von Partitionen unter Windows XP (NTFS)

11.1. Was ist Knoppix?

Auszug aus http://knopper.net/knoppix:

„ KNOPPIX is a bootable CD with a collection of GNU/Linux (http://www.linux.com/) software, automatic hardware detection, and support for many graphic cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk. “

11.2. Systemanforderungen

Bevor Sie LinuxDefender booten stellen Sie bitte sicher, dass Ihr System die folgenden Vorraussetzungen erfüllt:

Prozessortyp
X86 kompatibel mit einem Minimum von 166 MHz, aber bitte erwarten Sie in diesem Falle keine zufrieden stellende Systemleistung. Eine i686 Prozessorgeneration mit 800 MHz wäre die bessere Wahl.

Speicher
Die mindestens benötigte Speichergröße liegt bei 64 MB, für eine bessere Systemleistung wird jedoch 128 MB empfohlen.

CD-ROM
CD-Rom-Laufwerk und die BIOS-Einstellungen, um von CD zu booten.

Internetverbindung
Obwohl LinuxDefender auch ohne Internetverbindung lauffähig ist, benötigen die Update-Vorgänge eine aktive HTTP-Verbindung oder durch einen Proxy Server. Daher ist für einen aktuellen Schutz eine Internetverbindung ein MUSS.

Grafische Auflösung
800x600 für die web-basierte Administration.

11.3. Integrierte Software

Die Bitdefender Notfall CD enthält die folgenden Software-Pakete.

- BitDefender SMTP Proxy (AntiSpam & AntiVirus)
- BitDefender Remote Admin
- BitDefender Linux Edition (AntiVirus) + GTK Interface
- BitDefender Documentation (PDF- & HTML-Format)
- BitDefender Extras (Artwork, Leaflets)
- Linux-Kernel 2.6

- Captive NTFS write project
- LUFS - Linux Userland File System
- Werkzeuge zur Datenwiederherstellung
- Netzwerk- und Sicherheits-Analyse Werkzeuge für Administratoren
- Amanda Backup Lösung
- thttpd Tiny HTTP Daemon (Web-Server)
- Ethereal (Netzwerkdatenverkehrs-Analyse)
- Nessus (Netzwerkdatenverkehrs-Analyse)
- Parted, QTParted und Partimage (Partitionierungs-Werkzeuge)
- Adobe Reader (Zur Anzeige von PDF-Dokumenten)
- Mozilla Firefox Web Browser

11.4. BitDefender Lösungen für Linux

Die LinuxDefender Notfall CD beinhaltet die BitDefender SMTP Proxy Lösung für Linux mit integriertem AntiVirus/AntiSpam, BitDefender Remote Admin (einer web-basierten Verwaltungsoberfläche) und einer BitDefender Linux Edition (On-Demand Kommandozeilen-Scanner).

11.4.1. BitDefender SMTP Proxy

BitDefender für Linux Mail Server – SMTP Proxy ist eine Content-Inspection-Lösung, welche neben dem Schutz vor Viren zusätzlich AntiSpam-Funktionalitäten beinhaltet. Beide Schutzvarianten arbeiten direkt auf Gateway-Ebene, um somit den gesamten E-Mail-Datenverkehr zu überprüfen und effektiv sichern zu können. Durch die Verwendung fortschrittlichster Technologien ist BitDefender für Linux Mail Server mit allen gängigen E-Mail-Servern kompatibel und erhielt außerdem die Zertifizierung „Red Hat Ready“.

Die AntiVirus- und AntiSpam-Lösungen überprüfen, desinfizieren und filtern E-Mails auf allen gängigen E-Mail-Servern und auf nahezu jeder Betriebssystem-Plattform. BitDefender für Linux Mail Server – SMTP Proxy wird direkt beim Bootvorgang gestartet und überprüft alle eingehenden E-Mails. Um das Produkt zu konfigurieren, kann BitDefender Remote Admin eine web-basierte Konfigurationsschnittstelle verwenden.

11.4.2. BitDefender Remote Admin

Die BitDefender-Dienste können sowohl lokal als auch extern verwaltet werden. Gehen Sie hierzu bitte wie folgt vor:

1. Starten Sie den Firefox Web-Browser und öffnen Sie die Internetadresse: https://localhost:8139 (oder klicken Sie bitte doppelt auf das BitDefender Remote Admin Symbol auf Ihrem Desktop)
2. Melden Sie sich mit dem Benutzer „bd“ und dem Kennwort „bd“ am System an
3. Wählen Sie „SMTP Proxy“ aus dem linken Menü
4. Tragen Sie den „echten“ SMTP-Server und den Port ein
5. Fügen Sie E-Mail-Domains zum Relaying hinzu
6. Fügen Sie Netzwerk-Domains zum Relaying hinzu
7. Wählen Sie „AntiSpam“ aus dem linken Menü aus, um diese Funktionalität zu konfigurieren
8. Wählen Sie „AntiVirus“ aus dem linken Menü aus, um diese Funktionalität zu konfigurieren
9. Zusätzlich können Sie per „Mail Notifications“ die Benachrichtigungen konfigurieren

11.4.3. BitDefender Linux Edition

Der AntiViren-Scanner von BitDefender Linux Edition integriert sich direkt auf den Linux Desktop. Diese Version des Produkts beinhaltet eine auf GTK+ basierende grafische Benutzeroberfläche, über die der Prüfvorgang durchgeführt werden kann.



Wählen Sie in der Benutzeroberfläche einfach den zu überprüfenden Pfad bzw. das Laufwerk aus und klicken Sie mit der rechten Maustaste auf das jeweilige Objekt. Wählen Sie nun aus dem Kontextmenü den Eintrag „Scan with BitDefender“. Der Prüfvorgang wird nun gestartet und der Status des Prüfvorgangs inkl. eines abschließenden Berichts wird angezeigt. Für die Option Feineinstellungen lesen Sie bitte in der Linux Edition Dokumentation (in dem BitDefender Verzeichnis für Dokumentation oder entsprechenden Handbuchseite) und dem **/opt/BitDefender/lib/bdc** Programm nach.



12. LinuxDefender Kurzanleitung

12.1. Starten und Beenden

12.1.1. LinuxDefender starten

Um von der CD-ROM starten zu können, müssen Sie zunächst das BIOS Ihres Computers so konfigurieren, dass die Bootreihenfolge folgendermaßen aussieht: CD-ROM Laufwerk, Floppy-Laufwerk, Festplatte.

Starten Sie nun Ihren Computer neu und warten Sie, bis der initiale Bootvorgang abgeschlossen wurde. Sie bekommen nun den LinuxDefender Startbildschirm angezeigt. Folgen Sie nun bitte den angegebenen Schritten, um LinuxDefender zu starten.



LinuxDefender Startbildschirm

Drücken Sie `F2` um die erweiterten Einstellungen anzuzeigen. Drücken Sie bitte die Taste `F3` für die erweiterten Einstellungen in deutscher Sprache. Drücken Sie bitte die Taste `F4` für die erweiterten Einstellungen in französische Sprache. Drücken Sie bitte die Taste `F5` für die erweiterten Einstellungen in spanische Sprache. Um das System direkt zu starten, drücken Sie bitte die Taste `ENTER`.

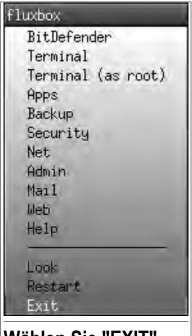
Sobald der Bootvorgang abgeschlossen wurde, wird der LinuxDefender Desktop angezeigt. Sie können nun damit beginnen, LinuxDefender zu verwenden.



Der LinuxDefender Desktop

12.1.2. LinuxDefender beenden

Um LinuxDefender ornungsgemäß zu beenden wird empfohlen alle Partitionen mit dem Befehl zu schließen **umount** oder klicken Sie per Rechtsklick auf das jweilige Festplatten Symbol auf dem Desktopund wählen Sie **Unmount**. Danach können Sie den Computer sicher herunterfahren indem Sie im Linux Defender Menü auf **Exit** klicken. (öffnen mit rechter Maustaste) oder indem Sie den Befehl **halt** im Terminal eingeben.



Wählen Sie "EXIT"

Sobald LinuxDefender alle Programme beendet hat, bekommen Sie eine textbasierte Ausgabe angezeigt. Sobald der Satz **Please remove CD, close cd-rom drive and hit return** angezeigt wird, können Sie die CD aus dem Laufwerk entfernen, den Einschub schließen und die Taste `ENTER` betätigen. Der Computer führt nun einen Neustart mit Ihrem bevorzugten Betriebssystem durch.



```
X-Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Sent all processes the TERM signal....................
Sent all processes the KILL signal....................
Shutting down network device eth0
Unmounting file systems.
/proc/bus/usb umounted
/ramdisk umounted
could not umount /KNOPPIX - trying /dev/cloop instead
/dev/root umounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return.
```

Warten auf diese Nachricht, wenn der Rechner heruntergefahren wird

12.2. Internetverbindung konfigurieren

Falls Sie über ein Netzwerk mit DHCP-Funktionalität verfügen und eine Netzwerkkarte in Ihrem Computer installiert ist, sollte LinuxDefender die notwendigen Einstellungen automatisch erkennen. Für eine manuelle Konfiguration folgen Sie bitte den folgenden Schritten.

1. Öffnen Sie per Rechtsklick auf den Desktop das Kontextmenü und wählen Sie **Terminal**.
2. Geben Sie **netcardconfig** als Befehl ein und drücken Sie die Taste ENTER.
3. Falls Sie DHCP in Ihrem Netzwerk verwenden, wählen Sie bitte **yes**.
4. Die Netzwerkkonfiguration sollte nun automatisch erkannt werden. Mit dem **ifconfig** können Sie Ihre IP Adresse und Netzwerkkarteneinstellungen einsehen.
5. Falls Sie eine statische IP-Adresse verwenden (kein DHCP), wählen Sie stattdessen **No**.
6. Folgen Sie den Instruktionen auf dem Bildschirm und konsultieren Sie Ihren Administrator.

Sollten diese Schritte erfolgreich abgeschlossen haben, können Sie die Verbindung folgendermaßen überprüfen. Geben Sie dazu den folgenden Befehl in das Terminal ein und drücken Sie ENTER.

```
$ ping -c 3 bitdefender.com
```

Falls Sie eine Einwahlverbindung verwenden, wählen Sie bitte **pppconfig** vom LinuxDefender Administrationsmenü. Folgen Sie bitte dann den Bildschirminstruktionen, um die PPP Internet Verbindung einzustellen.

12.3. BitDefender per Update aktualisieren

Die BitDefender Pakete für die LinuxDefender verwenden den Festplattenspeicher des Systems für erneuerbare Dateien. Über diesen Weg können Sie die neuen Virensignaturen, Prüfmaschinen oder die AntiSpam Datenbank aktualisieren. Dies geschieht sogar, wenn das System über Read only Medien, wie z.B. LinuxDefender CD, arbeitet.

Stellen Sie bitte zunächst sicher, ob Ihre Internetverbindung funktioniert. Öffnen Sie nun BitDefender Remote Admin und wählen Sie im linken Menü **Live! Update**. Klicken Sie nun auf die Schaltfläche **Update Now**, um das Update durchzuführen.

Alternativ können Sie auch ein Update über das Terminal durchführen. Dazu verwenden Sie bitte den folgenden Befehl.

```
# /opt/BitDefender/bin/bd update
```

Sämtliche Updatevorgänge werden in einer Berichtsdatei protokolliert. Diese können Sie mit dem folgenden Befehl im Terminal einsehen.

```
# tail  -f /ramdisk/BitDefender/var/log/bd.log
```

Falls Sie einen Proxy-Server zum Herstellen einer Internetverbindung verwenden, müssen Sie diesen Server zunächst im BitDefender Remote Admin, im Bereich **Live! Update** über die Schaltfläche **Configuration** angeben.

12.4. Prüfvorgänge durchführen

12.4.1. Wie erhalte ich Zugriff auf meine Daten unter Windows?

NTFS Schreibzugriff

Der NTFS Schreibzugriff wird über das Captive NTFS write project realisiert. Um diesen Zugriff zu verwenden, benötigen Sie die folgenden Dateien Ihrer Windows-Installation: `ntoskrnl.exe` und `ntfs.sys`. Derzeit werden nur Windows XP Treiber unterstützt. Sie können diese Treiber jedoch auch dazu verwenden, um auf Partitionen von Windows NT 4.0, 2000 und 2003 zu zugreifen. Für Windows 98 und ME werden keinerlei Treiber zum Schreibzugriff benötigt.

Installieren der NTFS Treiber

Um einen Zugriff zu Ihren Windows-Partitionen mit NTFS-Dateisystem zu erhalten und auf diesen schreiben zu können, müssen Sie zunächst die NTFS Treiber installieren. Wird dieser Schritt nicht durchgeführt, erhalten Sie nur schreibgeschützten Zugriff. Falls Sie FAT und nicht NTFS für Ihre Windows Partitionen verwenden oder lediglich einen Lesezugriff für Ihre Daten benötigen, können Sie die Laufwerke direkt einbinden und somit einen Zugriff auf Windows Laufwerke erhalten, als wären es Linux Laufwerke.

Um die Schreibunterstützung zu erhalten, speichern Sie die NTFS Treiber auf Ihrer lokalen Festplatte, entfernte Netzlaufwerke, einen USB Stick oder beziehen Sie diese Treiber direkt über das Windows Update. Es wird empfohlen, nicht die Treiber der verwendeten Windows-Installation einzusetzen, da diese im Falle einer Infizierung durch einen Virus ggf. ebenfalls beschädigt sind und nicht korrekt funktionieren.

Klicken Sie doppelt auf das Desktop-Symbol **Install NTFS Write Drivers**, um den Installationsvorgang zu starten. Wählen Sie die erste Option, wenn Sie die Treiber von der lokalen Festplatte installieren möchten.

Haben Sie die Treiber an einem anderen Ort gespeichert, wählen Sie bitte **Quick search** aus, um nach den Treiber suchen zu lassen.

Alternativ können Sie selbst einen Speicherort angeben oder die Treiber direkt über den Download des Service Pack 1 für Windows XP beziehen.

Die Treiber werden nicht auf Ihrer Festplatte installiert, sondern lediglich temporär von LinuxDefender verwendet, um auf die NTFS-Partitionen zu zugreifen. Sofern das Programm die Treiber installiert hat, können Sie die entsprechenden Partitionen per Doppelklick aufrufen und deren Inhalt einsehen. Für einen wirkungsvollen Datei Manager verwenden Sie bitte den Midnight Commander von dem LinuxDefender Menü (oder geben Sie **mc** in der Konsole ein).



12.4.2. Wie führe ich einen Prüfvorgang durch?

Wählen Sie die gewünschten Ordner aus und klicken Sie per Rechtsklick auf diese. Wählen Sie nun aus dem Kontextmenü den Eintrag **Send to** und klicken Sie nun auf **BitDefender Scanner**.

Alternativ kann der Prüfvorgang auch mit Rechten des Benutzers root über den Terminal durchgeführt werden. Geben Sie dazu den folgenden Befehl im Terminal ein und bestätigen Sie mit der Taste ENTER.

```
# /opt/BitDefender/bin/bdgtk2 /path/to/scan/
```

Klicken Sie nun in der Benutzeroberfläche auf **Start Scan**.

Falls Sie weitere Einstellungen vornehmen möchten, klicken Sie zuvor bitte auf **Configure Antivirus**.

12.5. Erstellen einer Ad-Hoc Mail-Filterungs-Lösung

Sie können LinuxDefender dazu benutzen eine Ad-Hoc Mail-Filter-Lösung zu erstellen, ohne dass Sie eine Software installieren oder den E-Mail-Server modifizieren müssen. Die Idee dahinter ist, dass Sie ein LinuxDefender System vor Ihrem Mail-Server benutzen und BitDefender erlauben, jeden SMTP-Verkehr nach Spam und Viren zu scannen und ihn anschließend gefiltert an den Mail-Server weiterzugeben.

12.5.1. Vorbereitende Maßnahmen

Sie benötigen mindestens einen Computer mit einer Pentium 3-kompatiblen CPU, 256 MB RAM und ein CD/DVD-Laufwerk, um davon zu starten. LinuxDefender muss den SMTP-Verkehr anstelle des eigentlichen E-Mail-Server bekommen. Es gibt verschiedene Wege um dies einzustellen.

1. Ändern Sie die IP des eigentlichen Mail-Servers und vergeben die alte IP an das LinuxDefender System
2. Ändern Sie Ihre DNS-Einträge, sodass der MX-Eintrag für Ihre Domains zu dem LinuxDefender System zeigt
3. Stellen Sie Ihre Mail-Clients auf das neue LinuxDefender System als SMTP-Server ein
4. Ändern Sie Ihre Firewall-Einstellungen so ab, dass alle SMTP-Serververbindungen an LinuxDefender weitergeleitet werden, anstatt an den eigentlichen Mail-Server

Das Linux How To wird die obigen Anweisungen nicht erklären. Für weitere Informationen konsultieren Sie bitte Linux Networking guides und Netfilter documentation.

12.5.2. Der Mail-Filter

Starten Sie Ihre LinuxDefender CD-ROM und warten Sie, bis das X Windows-System geladen ist.

Um den BitDefender SMTP-Proxy zu konfigurieren, doppelklicken Sie auf das **BitDefender Remote Admin** Symbol auf dem Desktop. Ein weiteres Fenster wird erscheinen. Benutzen Sie als Benutzernamen und als Kennwort `bd`, um sich anzumelden.

Nach dem erfolgreichen Login bekommen Sie die Möglichkeit, den BitDefender SMTP-Proxy zu konfigurieren.

Wählen Sie **SMTP Proxy** aus, um den eigentlichen Mail-Server einzutragen, den Sie vor Viren und Spam schützen möchten.

Klicken Sie auf die Kategorie **Email domains**, um alle Domains einzugeben, von denen Sie E-Mails akzeptieren möchten.

Wählen Sie **Add Email Domain** oder **Add Bulk Domains** und folgen den Anweisungen, um die Relays einzustellen.

Wählen Sie die Kategorie **Net domains**, um alle Netzwerke einzugeben, die Sie relayen möchten.

Wählen Sie **Add Net Domain** oder **Add Bulk Net Domains** und folgen den Anweisungen um die Relays einzustellen.

Wählen Sie **Antivirus** aus dem linken Menü, um auszuwählen was zu tun ist, wenn ein Virus gefunden wird, und um andere AntiVirus-Optionen zu konfigurieren.

Nun wird der gesamte SMTP-Verkehr von BitDefender gescannt und gefiltert. Standardmäßig werden alle virusinfizierte Mails gesäubert und alle Spam E-Mails von BitDefender werden im Betreff der Mail mit dem Wort `[SPAM]` gekennzeichnet. Ein E-Mail-Header (`X-BitDefender-Spam: Yes/No`) wird zu jeder Mail hinzugefügt, um die client-seitige Filterung zu erleichtern.

12.6. Eine Netzwerk-Sicherheitsprüfung durchführen

Neben den Möglichkeiten der Erkennung von Schädlingen und dem Filtern von Emails ist es mit LinuxDefender auch möglich, Ihr Netzwerk einer Sicherheitsprüfung zu unterziehen. Für diesen Fall sind Computer-forensische Werkzeuge auf dieser CD-ROM enthalten, mit denen es möglich ist, kompromittierte Systeme zu überprüfen und das Netzwerk auf Eindringlinge zu untersuchen. Bitte lesen Sie diese kurze Einführung, um mehr darüber zu erfahren, wie man eine kurze Prozessanalyse der Server und des Netzwerks vornimmt.

12.6.1. Auf Rootkits überprüfen

Bevor Sie Ihr Netzwerk einer solchen Prüfung unterziehen, sollten Sie zunächst sicherstellen, dass der Host, von dem Sie die Prüfung durchführen, nicht kompromittiert wurde. Starten Sie hierfür zunächst einen Prüfvorgang mit BitDefender. Sie können einen Prüfvorgang für die installierten Festplatten vornehmen, beschrieben in der Einführung für **Scan for viruses**, oder Sie können auf Unix rootkits (ähnlich zu trojanischen Pferden) prüfen.

Überprüfen Sie nun, ob eventuelle Eindringlinge einen Rootkit (eine Art Hintertür) auf dem System installiert haben. Zu diesem Zwecke wird das Programm **ChkRootKit** mitgeliefert. Um bestimmte Festplatten mittels diesem Programm zu überprüfen, verwenden Sie bitte den folgenden Befehl im Terminal und bestätigen Sie diesen anschließend mit der Taste ENTER. `-r NEWROOT` Parameter um das das neue (root) Verzeichnis auf dem Host zu definieren.

```
# chkrootkit -r /dev/hda3
```

Wird ein Rootkit gefunden, so zeigt das Programm diese Ausgabe in **fetter Schrift** im Terminal an.

12.6.2. Nessus – der Netzwerk Scanner

> Nessus ist die beliebteste Open-Source Software zum Entdecken von Sicherheitslücken in Netzwerken und wird von über 75.000 Unternehmen weltweit eingesetzt. Nessus kann dazu eingesetzt werden, remote das Netzwerk auf verschiedenste Sicherheitslücken zu überprüfen und schlägt diverse Verbesserungsvorschläge vor, um das Netzwerk zu sichern und das Risiko eines Einbruchs zu minimieren.
>
> —*www.nessus.org*

Nessus ist die beliebteste Open-Source Software zum Entdecken von Sicherheitslücken in Netzwerken und wird von über 75.000 Unternehmen weltweit eingesetzt. Nessus kann dazu eingesetzt werden, remote das Netzwerk auf verschiedenste Sicherheitslücken zu überprüfen und schlägt diverse



Verbesserungsvorschläge vor, um das Netzwerk zu sichern und das Risiko eines Einbruchs zu minimieren.

Klicken Sie doppelt auf das Desktop-Symbol **Nessus Security Scanner** oder starten Sie das Programm über den Befehl **startnessus** im Terminal. Warten Sie nun bis das Fenster angezeigt wird. Dies kann je nach Hardware-Konfiguration 5 bis 10 Minuten andauern, da die Software über 5.000 Plug-Ins beinhaltet. Verwenden Sie den Benutzer `knoppix` und das Kennwort `knoppix` um sich anzumelden.

Klicken Sie auf den Abschnitt **Target selection** und geben Sie die IP-Adressen bzw. Hostnamen der Computer an, die Sie auf mögliche Sicherheitslücken überprüfen möchten. Stellen Sie danach sicher, dass die Prüfoptionen gemäß den Gegebenheiten in Ihrem Netzwerk angepasst sind. Somit können Sie Ressourcen und Bandbreite einsparen und erhalten ein akkurateres Prüfergebnis. Klicken Sie nun auf **Start the scan** um den Prüfvorgang zu starten.

Nach Abschluss des Prüfvorgangs erhalten Sie einen ausführlichen Bericht des Programms angezeigt, welcher Sie auf Schwachstellen hinweist und entsprechende Empfehlungen zu diesen bereitstellt. Der gespeicherte Bericht kann in dem von Ihnen bevorzugten Browser eingesehen werden.

12.7. Den Arbeitsspeicher (RAM) Ihres Computers überprüfen

Sollte Ihr Computer des Öfteren unerwartet abstürzen oder sog. „Blue Screens“ anzeigen, empfehlen wir Ihnen, den Arbeitsspeicher (RAM) Ihres Computers zu überprüfen. Dies können Sie ebenfalls mittels der LinuxDefender Notfall CD durchführen. Gehen Sie hierzu bitte wie folgt beschrieben vor.

Starten Sie Ihren Computer von der LinuxDefender CD und warten Sie, bis die den Startbildschirm mit erweiterten Einstellungsmöglichkeiten angezeigt bekommen. Tippen Sie nun den Befehl **memtest** ein und bestätigen Sie diesen mit drücken der Tast ENTER.

Das Programm zum Überprüfen des Arbeitsspeichers startet nun automatisch und überprüft diesen in mehreren Durchgängen. Sie können die Einstellungen des Speichertests jederzeit durch Drücken der Taste `c` auf Ihrer Tastatur beliebig anpassen.

Ein vollständiger Test des Arbeitsspeichers benötigt circa 8 Stunden, abhängig von der Kapazität und Geschwindigkeit des Speichers. Es wird empfohlen, diesen Test komplett durchlaufen zu lassen, er kann jedoch jederzeit durch drücken der Taste `ESC` auf Ihrer Tastatur abgebrochen werden.

Falls Sie vor kurzem neuen Arbeitsspeicher erworben haben, empfehlen wir Ihnen diesen einmal mittels dieser Methode zu überprüfen, um eventuelle Produktionsfehler noch vor Ablauf der Garantie zu erkennen und somit Systemabstürze und Datenverlust zu vermeiden.



13. Support

13.1. Technische Beratung

Als eines der führenden Dienstleistungsunternehmen für IT Sicherheitslösungen möchten wir Ihnen eine möglichst schnelle, kompetente und unkomplizierte technische Unterstützung bei auftretenden Fragen anbieten.Unser technischer Support ist zu diesem Zweck stets mit den aktuellsten Virensignaturen, neuesten Informationen und präzisen Antworten auf wiederkehrende Fragen ausgestattet.

Insbesondere zeichnet sich SOFTWIN durch ein hohes Maß an Innovation, ein hervorragendes Preis-Leistungsverhältnis und eine kurze Reaktionszeit in allen Belangen aus.Kundenzufriedenheit ist für uns nicht nur eine Floskel, sondern Firmenphilosophie.Es ist jedoch leider nicht vollkommen auszuschließen, dass es bei der Bearbeitung Ihrer Anfragen zu Engpässen kommen kann und bitten diesbezüglich um Nachsicht.

Wir freuen uns auf die Kontaktaufnahme zu unseren technischen Support und stehen Ihnen mit Rat und Tat zur Seite. Nutzen Sie hierfür einfach unseren E-Mail Kontakt `<support@bitdefender.de>` oder rufen Sie uns Werktags unter (075 42) 94 44-60 an.Falls Sie den Weg über E-Mail bevorzugen, teilen Sie uns bitte mit, welches Produkt und Betriebssystem Sie verwenden und beschreiben Sie das aufgetretene Problem so detailliert als möglich.

13.2. Online-Hilfe

13.2.1. BitDefender Knowledge Base

Bei der BitDefender Knowledge Base handelt es sich um eine Wissensdatenbank mit Informationen und hilfreichen Tipps & Tricks rund um die Produkte.In leicht verständlicher Form bietet die Knowledge Base Informationen, Anleitungen und Berichte über neue Patches und behobene Probleme.Ebenfalls enthalten sind empfohlene Vorgehensweisen bei der Verwendung von Produkten und allgemeine Informationen wie z.B. Präventionsmaßnahmen vor Viren und anderen Schädlingen.

Die BitDefender Knowledge Base ist zudem öffentlich zugänglich und komplett durchsuchbar.Durch diese Art der Informationsbereitstellung bieten wir unseren Kunden eine weitere Möglichkeit, technische Grundlagen und Fachwissen über unsere Produkte zu erlangen.

Die BitDefender Knowledge Base ist jederzeit unter der Internet-Adresse http://kb.bitdefender.de erreichbar.

13.3. Kontaktinformationen

Effiziente und kundenorientierte Kommunikation ist der Schlüssel zu einem erfolgreichen Geschäftsmodell.Seit mehr als 10 Jahren überbietet SOFTWIN konstant die bereits hochgesteckten Erwartungen unserer Kunden und Partner und diese Tradition wollen wir auch in Zukunft fortführen.

13.3.1. Kontaktadressen

Vertrieb: `<vertrieb@bitdefender.de>`
Technische Beratung: `<support@bitdefender.de>`
Falls Sie dennoch Fehler finden, so teilen Sie uns diese bitte mit indem Sie uns per E-Mail unter der Adresse `<documentation@bitdefender.com>` kontaktieren.
Vertrieb: `<vertrieb@bitdefender.de>`

Vertrieb: <vertrieb@bitdefender.de>
<presse@bitdefender.de>
Jobs: <jobs@bitdefender.com>
Virus-Einsendungen: <virus_submission@bitdefender.com>
Spam-Einsendungen: <spam_submission@bitdefender.com>
Viren melden: <abuse@bitdefender.com>
Webseite: http://www.bitdefender.de
Webseite: http://www.bitdefender.de
Lokale Anbieter: http://www.bitdefender.de
BitDefender Knowledge-Base: http://kb.bitdefender.de

13.3.2. Niederlassungen

Die BitDefender Niederlassungen stehen für Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung, sowohl für vertriebliche als auch für allgemeine Anfragen. Die genauen Kontaktdaten und Adressen finden Sie in der unten stehenden Auflistung.

Deutschland

Softwin GmbH
Headquarter Western Europe
Karlsdorferstrasse 56
88069 Tettnang
Deutschland
Phone: +49 (0)75 42 -94 44 44
Fax: +49 (0)75 42 - 94 44 99
<support@bitdefender.de>
Vertrieb: <vertrieb@bitdefender.de>
Web: http://www.bitdefender.de
Technische Beratung: <support@bitdefender.de>

Großbritannien und Irland

One Victoria Square
Birmingham
B1 1BD
Phone: +44 207 153 9959
Fax: +40 21 - 233 07 63
<support@bitdefender.de>
Vertrieb: <vertrieb@bitdefender.de>
Web: http://www.bitdefender.de
Technische Beratung: <support@bitdefender.de>

Spain

Constelación Negocial, S.L
C/ Balmes 195, 2ª planta, 08006
Barcelona
Soporte técnico: <soporte@bitdefender-es.com>
Ventas: <comercial@bitdefender-es.com>
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com



U.S.A.

BitDefender LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33308
Technical support:
<support@bitdefender.com>
Customer Service: 954-776-6262
http://www.bitdefender.com

Romania

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Technical support: <suport@bitdefender.ro>
Sales: <sales@bitdefender.ro>
Phone: +40 21 2330780
Fax: +40 21 2330763
Product web site: http://www.bitdefender.ro



Glossar

ActiveX

ActiveX ist ein Programmuster, dass von anderen Programmen und Betriebssystemkomponenten unter Windows aufgerufen werden kann. Die ActiveX Technologie wird von Microsofts Internet Explorer benutzt, damit interaktive Webseiten eher wie Programme und nicht wie statische Seiten angezeigt werden. Mit ActiveX können die Benutzer z.B. Fragen stellen oder beantworten, Buttons verwenden, oder verschiedenartige Interaktionen mit der Webseite herstellen. ActiveX-Steuerelemente werden oft in Visual Basic geschrieben.

Erwähnenswert ist, dass bei ActiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, ActiveX über das Internet zu nutzen.

Adware

Adware ist häufig mit einer Absenderanwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware Anwendungen müssen in der Regel installiert werden, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

Archiv

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einer Datensicherung/BackUp erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

Backdoor (Hintertür)

Eine Sicherheitslücke eines Systems, die der Entwickler oder Verwalter absichtlich hinterlässt. Der Grund dafür muss nicht immer bösartig sein. Manche Betriebssysteme haben schon bei der Fabrikation privilegierte Konten, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Bootsektor

Der erste Sektor einer Festplatte oder Diskette. Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

Bootvirus

Ein Virus, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert. Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird dieser im Arbeitsspeicher aktiviert. Bei jedem Neustart wird der Virus so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

Browser

Kurzform für Web-Browser, eine Softwareanwendung, die zum Lokalisieren und Anzeigen von Webseiten verwendet wird. Die bekanntesten Browser sind Netscape Navigator und Microsoft Internet Explorer. Beide sind graphische Browser, das heißt sie können sowohl Grafiken als auch Texte anzeigen.Weiterhin können die meisten Browser Multimedia-Informationen wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

Befehlszeile

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur

benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

Cookie

In der Internetindustrie werden Cookies als kleine Dateien beschrieben, die Daten über einzelne Computer enthalten und die von den Werbern analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden.Die Cookie-Technologie wurde deshalb weiter entwickelt, damit der Benutzer nur solche Werbung zugeschickt bekommt, die seinen Interessen dient.Für viele ist es aber wie ein zweischneidiges Messer.Einerseits ist es wirksam und sachbezogen, da man nur Anzeigen, an denen man interessiert ist, betrachten kann, anderseits heißt es dem Benutzer "auf die Spur zu kommen" und ihn auf Schritt und "Klick " zu verfolgen.Es ist verständlich, dass der Datenschutz ein umstrittenes Thema ist und viele sich von dem Begriff als SKU-Nummern (die Streifencodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden, angegriffen fühlen.Auch wenn dieser Gesichtspunkt extrem erscheint ist er manchmal korrekt.

Laufwerk

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann.

Ein Festplatten-Laufwerk liest und beschreibt Festplatten.

Ein Disketten-Laufwerk liest und beschreibt Disketten.

Laufwerke können sowohl interner (im Rechner eingebaut) als auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.

Download (Herunterladen)

Kopiert Daten (gewöhnlich eine ganze Datei) von einer Hauptquelle auf ein Peripheriegerät. Der Begriff bezeichnet oft den Kopiervorgang von einem Online Service auf den eigenen Rechner. Download oder Herunterladen kann auch das Kopieren einer Datei von einem Netzwerkserver auf einen Netzwerkrechner bedeuten.

E-Mail

Elektronische Post.Ein Dienst, der Nachrichten an andere Rechner über ein lokales oder ein globales Netzwerk übermittelt.

Ereignis

Ereignisse oder Erscheinungen, die in einem Programm vorkommen. Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

Fehlalarm

Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist. Kann bei heuristischem Virenprüfen auftreten.

Dateierweiterung

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS. Sie enthalten gewöhnlich ein bis zwei Buchstaben (alte Betriebssysteme können nicht mehr als drei Buchstaben unterstützen), Beispiele dafür sind "c" für C-Quellcode, "ps" für PostScript oder "txt" für beliebige Texte. Windows zeigt bei ihm bekannten Dateitypen keine Dateierweiterung in der graphischen Benutzeroberfläche an, stattdessen wird häufig ein Symbol verwendet.

Heuristik

Eine Methode, um neue Viren zu identifizieren. Diese Prüfmethode beruht nicht auf spezifische Virussignaturen. Der Vorteil einer heuristischen Prüfung ist, dass man nicht von einer neuen Virusvariante getäuscht werden kann. Manchmal kann auch ein verdächtiger Code in einemnormalen Programm gemeldet werden, ein sogenannter Fehlalarm wird angezeigt.



IP

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

Java Applet

Ein Java Programm, das nur auf Webseiten läuft. Um ein Applet auf einer Webseite zu benutzen, gibt man den Namen und die Größe (Länge und Breite in Pixel) des Applets an. Wenn die Webseite abgerufen wird, lädt der Browser das Applet vom Server herunter und führt es auf der Benutzermaschine (dem Client) aus. Applets sind keine Anwendungen, da sie von strengen Sicherheitsprotokollen gesteuert werden.

Obwohl Applets auf dem Client laufen, können diese keine Daten auf der Clientmaschine lesen oder schreiben. Zusätzlich sind die Applets weiter begrenzt, so dass sie nur Daten aus der Domäne lesen und beschreiben können, die sie unterstützen.

Makrovirus

Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen mächtige Makrosprachen.

Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird.Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

E-Mail Client

Ein E-Mail Client ist eine Anwendung, die das Senden und Empfangen von E-Mails ermöglicht.

Arbeitsspeicher

Interne Speicherzonen im Rechner. Der Begriff Arbeitsspeicher bedeutet Datenträger in Form von sehr schnellen Chips. Das Wort Speicher ist der Speicherplatz, der sich auf Magnetbändern oder Datenträgern befindet. Jeder Rechner hat eine gewisse Menge Arbeitsspeicher.Dieser wird auch Hauptspeicher oder RAM genannt.

Nicht heuristisch

Diese Prüfmethode beruht auf einer spezifischen Virussignatur. Der Vorteil einer nicht heuristischen Prüfung ist, dass diese nicht von einem Scheinvirus getäuscht werden kann, und dass dieser keinen falschen Alarm auslöst.

Komprimierte Programme

Eine Datei in einem komprimierten Format. Viele Betriebssysteme und Anwendungen enthalten Befehle, die das Komprimieren einer Datei ermöglichen, so dass diese weniger Speicherplatz benötigt. Zum Beispiel: Angenommen Sie haben einen Text, der 10 aufeinander folgende Leerzeichen enthält. Normalerweise nehmen diese 10 Bytes Speicherplatz ein.

Ein Programm, das Dateien komprimiert, würde die Leerzeichen durch ein spezielles Zeichen „Leerzeichenreihe“ ersetzen, gefolgt von der Zahl der Leerzeichen, die ersetzt wurden. In diesem Fall sind nur noch zwei Bytes notwendig statt zehn. Das wäre ein Beispiel für eine Komprimierungstechnik, es gibt aber noch viele andere.

Pfad

Zeigt die Stelle an, an der sich eine Datei in einem Rechner befindet. Diese Pfadangaben enthalten gewöhnlich den hierarchischen Aufbau des Dateiverzeichnisses: Laufwerke, Ordner, Unterverzeichnisse, die Datei und ihre Erweiterung.

Der Weg zwischen zwei Punkten, wie zum Beispiel der Kommunikationskanal zwischen zwei Rechnern.

Phishing

Dabei wird eine E-Mail mit einer betrügerischen Absicht an einen Nutzer gesendet.Der Inhalt dieser E-Mail gibt vor, von einem bekannten und seriös arbeitenden Unternehmen zu stammen. Zweck dieser E-Mail ist es dann, private und geheime Nutzerdaten zu erhalten, worauf der Absender beabsichtigt, die Identität des Nutzers anzunehmen. Die E-Mail führt den Benutzer

dann auf eine Webseite, in der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TAN's oder PIN's preiszugeben. Dies soll aus Gründen der Aktualisierung geschehen. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Polymorpher Virus
Ein Virus, der seine Form mit jeder Datei, die er infiziert, ändert. Da diese Viren kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Schnittstelle
Stelle eines Rechners, an die ein Gerät angeschlossen werden kann. Rechner haben verschiedenartige Schnittstellen. Intern gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen. Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen. Die Schnittstellennummer gibt die Art der Schnittstelle an. Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Logdatei (Berichtsdatei)
Eine Datei, die stattgefundene Aktivitäten aufzeichnet. Zum Beispiel speichert BitDefender eine Logdatei mit die geprüften Pfaden, Ordnern und der Archivanzahl, aber auch die geprüften, infizierten oder verdächtigen Dateien.

Rootkit
Bei einem Rootkit handelt es sich um einen Satz von Softwarewerkzeugen die einem Administrator Low-End Zugriff zu einem System verschaffen. Rootkits traten zunächst nur auf UNIX-Systemen auf und haben im Laufe der Zeit auch Ihren Einzug auf Linux- und Windows-Systemen gehalten.

Die Hauptaufgabe eines Rootkits besteht darin, seine Existenz zu verstecken indem Prozesse und Dateien versteckt werden, Anmeldedaten und Berichtsdateien zu fälschen und jegliche Art von Daten abzufangen.

Rootkits zählen von Haus aus nicht zu schadensverursachender Software da Sie keine Schadroutinen besitzen. Jedoch verändern Sie die vom Betriebssystem zurückgegebenen Daten und verstecken auf diese Weise ihre Präsenz. Dennoch kann über ein solches Rootkit schädliche Software nachträglich eingeschleust werden und auch der wirtschaftliche Schaden ist nicht zu unterschätzen.

Skript
Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam
Junk-E-Mail oder Junk-Postings in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware
Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten überwacht und über seine Internetverbindung abruft. Dies geschieht in der Regel zu Werbezwecken. Typischerweise werden Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Sharewareprogrammen gebündelt, die aus dem Internet herunter geladen werden können. Es ist jedoch darauf hinzuweisen, dass die Mehrzahl der Shareware- und Freeware-Anwendungen frei von Spyware ist. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an jemand anderen. Spyware kann auch Informationen über E-Mail-Adressen und sogar Kennwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Eine weit verbreitete Möglichkeit, ein Opfer von Spyware zu werden, ist der Download von bestimmten heute erhältlichen Peer-to-Peer-Dateiaustauschprogrammen (Direktverbindungen von Computern).



Abgesehen von den Fragen der Ethik und des Datenschutzes bestiehlt Spyware den Anwender, indem sie Speicherressourcen seines Rechners nutzt und den Internetzugriff verlangsamt, indem über seine Internetverbindung Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Startup Objekt (Autostart-Objekt)

Jede Datei, die sich in diesem Ordner befindet, öffnet sich, wenn der Rechner gestartet wird.Zum Beispiel ein Startbildschirm, eine Sounddatei, die abgespielt wird, wenn der Rechner gestartet wird, ein Erinnerungskalender oder Anwendungsprogramme können Autostart-Objekte sein. Gewöhnlich wird eine Alias-Datei (Verknüpfung) statt der eigentlichen Datei in diesen Ordner gelegt.

Systemleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Taskleiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Er enthält kleine Icons zur Information und zum leichteren Zugriff, zum Beispiel: Fax, Drucker, Modem, Lautstärke und mehr. Um auf die Details und Steuerungen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol - Im Internet werden eine Vielzahl von verschiedener Hardware und Betriebssystemen miteinander verbunden. TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Trojaner

Ein vernichtendes Programm, das sich als eine freundliche Anwendung tarnt und auftritt. Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können zerstörerisch sein. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert. Viele Trojaner öffnen den Rechner für den Zugriff von außen.

Der Begriff entstammt einer Geschichte in Homer's "Ilias", in der die Griechen Ihren Feinden, den Trojanern, angeblich als Sühnegabe ein hölzernes Pferd schenkten. Aber, nachdem die Trojaner das Pferd innerhalb der Stadtmauern gebracht hatten, kamen die in dem Bauch des hölzernen Pferdes versteckten Soldaten heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsmännern in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Update (Aktualisierung)

Neue Softwareversionen oder Hardwareprodukte, die eine ältere Version ersetzen. Die Update-Installationsroutine sucht nach älteren Versionen auf dem Rechner, da sonst kein Update installiert werden kann.

BitDefender hat sein eigenes Update Modul, welches das manuelle oder automatische Prüfen nach Updates ermöglicht.

Virus

Ein Programm oder ein Codestück, das auf einen Rechner geladen wird, ohne dass der Benutzer Kenntnis davon hat und welches sich allein ausführt. Die Resultate von Viren können einfache Scherzmeldungen aber auch die Zerstörung von Hardware sein. Die meisten Viren können sich selber vervielfältigen. Alle Computerviren sind von Menschenhand geschrieben. Ein Virus, der sich immer wieder vervielfältigen kann ist sehr einfach zu schreiben. Sogar ein solch einfacher Virus ist fähig, sich durch Netzwerke zu verschicken und Sicherheitssysteme zu überbrücken.

Virusdefinition

Ein binäres Virusmuster, das von einem AntiVirus Programm verwendet wird, um einen Virus zu entdecken und zu entfernen.

Wurm

Ein Programm, das sich über ein Netzwerk verbreitet. Es kann sich nicht an andere Programme anhängen.